# OS ATAQUES *RANSOMWARE* E A CAMADA DE PROTEÇÃO EM SISTEMAS GOVERNAMENTAIS

## ARTIGO DE REVISÃO

SANTOS, Levi Alves dos[1]

SANTOS, Levi Alves dos. **Os ataques *ransomware* e a camada de proteção em sistemas governamentais.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 07, Ed. 08, Vol. 04, pp. 132-161. Agosto de 2022. ISSN: 2448-0959, Link de acesso: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware, DOI: 10.32749/nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

## RESUMO

*Ransomware* é um *software* malicioso utilizado para sequestro e criptografia de dados pessoais, empresariais ou governamentais, seguindo-se a esse roubo/bloqueio um pedido de resgate por meio de criptomoeda, cujo rastreio é impossível. Como questão norteadora está a pergunta: quais são as boas práticas em Gestão de Sistemas em Tecnologia da Informação e como podem colaborar para mitigar os ataques *ransomware*? O objetivo deste artigo consiste em apresentar múltiplos casos de ataques *ransomware* aos sistemas eletrônicos de diferentes empresas de porte nos Estados Unidos e os meios preventivos existentes no presente para mitigação de tais riscos. O presente artigo original foi desenvolvido adotando como metodologia a pesquisa bibliográfica, para discorrer sobre programas eletrônicos maliciosos (*malwares*) no padrão explicado. As principais conclusões verificadas foram: necessidade da adoção das boas práticas relativas à segurança e gerenciamento de informação; investimentos em sistemas de segurança de alto nível para proteção de rede local ou remota; investimentos em profissionais especializados em Tecnologia da Informação e detentores de sólidos conhecimentos em *ransomware*; normatização dos usos e práticas no uso dos dispositivos organizacionais; elaboração e guarda de *backups* sistêmicos; conscientização de indivíduos e empresas sobre o não pagamento de resgates.

Palavras-chave: Ciberespaço, Crime cibernético, *Ransomware*.

## INTRODUÇÃO

A informação é, na atualidade, o recurso mais poderoso para indivíduos, organizações e instituições de estado. Segundo Brito (2016, p. 8), a informação, ao longo do tempo, passou a representar um importante capital no contexto das organizações, tanto quanto de instituições governamentais, e no âmbito pessoal. No que se refere ao âmbito comercial, o acesso indevido de terceiros a informações confidenciais de uma empresa pode levá-la ao fracasso em seu segmento de atuação mercadológico, assim como o financeiro.

Nesta perspectiva, o ciberespaço é uma estrutura cuja territorialidade vem sendo construída em nível global, a partir da Sociedade da Informação. Em sua dinâmica inserem-se as relações entre os espaços local e global, efetivadas por meio “das redes de informação e cooperação das mais variadas naturezas”, contando com sua estrutura física e o fluxo de informações possíveis para a formação e funcionamento das comunidades virtuais possibilitadas pela *internet* (SILVA, 2014).

Será apresentada a incidência de ataques *ransomware* de grandes proporções feitos a empresas norte-americanas a partir de 2017, a partir da apresentação dos diferentes casos, com e sem pagamento de resgate. Além disso, foram listados os diferentes tipos de *malwares* e efeitos que operam nos dispositivos de suas vítimas.

Como questão norteadora está a pergunta: quais são as boas práticas em Gestão de Sistemas em Tecnologia da Informação e como podem colaborar para mitigar os ataques *ransomware*?

O objetivo deste artigo consiste em apresentar múltiplos casos de ataques *ransomware* aos sistemas eletrônicos de diferentes empresas de porte nos

Estados Unidos e os meios preventivos existentes atualmente para mitigação de tais riscos.

A presente pesquisa bibliográfica trará uma breve linha do tempo relacionada ao surgimento da *internet,* ao avanço das Tecnologias da Informação e dispositivos, o surgimento e evolução de programas virtuais maliciosos, os maiores ataques cibernéticos ocorridos na última década contra empresas norte-americanas, e um rol de medidas de segurança que conjuntas, compõem as boas práticas neste segmento.

## O ADVENTO DA *INTERNET*

No intervalo entre 1947 e 1991 surge a Guerra Fria, conflito não armado, mas de caráter político-ideológico, entre as duas maiores potências mundiais, à época, os Estados Unidos da América (EUA) e a União Soviética (URSS), dividindo a aldeia global em dois grupos que representavam, respectivamente, o capitalismo e o comunismo (SILVA, 2022).

Naquele momento emerge a necessidade de uma comunicação ágil, segura e eficaz, que foi desenvolvida pela administração pública dos Estados Unidos para viabilizar a interligação entre universidades e centros de pesquisa (SILVA, 2022).

Nascia a *internet,* que veio a popularizar-se a partir dos anos 1990, mediante o surgimento das Tecnologias de Informação e Comunicação (TICs), que permitiram a digitalização progressiva dos diferentes tipos de materiais e documentos (SILVA, 2014), além de projetar os meios eletrônicos como uma nova opção de comunicação ágil na integração entre governos e cidadãos, mediante a “inovação, racionalização e adoção de modelos de gestão que priorizem a disponibilização de informações e serviços para os cidadãos" (MEDEIROS *et al*., 2020, p. 652).

Para Medeiros *et al*. (2020, p. 651), o ciberespaço detém o domínio das interações humanas, sendo um espaço artificial, porém, constituído por “peculiaridades

únicas, que se formou a partir da interligação de camadas físicas (pessoas e máquinas) com camadas digitais (*software* e informações)".

No que se refere à Sociedade da Informação, Marietto (2001) ensina que é composta não apenas por um determinado espaço físico delimitado, mas também por aquele vivenciado pelas comunidades, cujo ambiente de comunicação é justamente o ciberespaço.

Para definir tal conceito, Marietto (2001, p. 32) reporta a definição de Irvine (1998), quando explica tratar-se de "uma camada imaginária de redes situada no topo da estrutura física das cidades, camada essa que envolve o 'espaço material da economia e a infraestrutura global'", mencionando que a composição desse espaço material também se dá pelo telefone, telégrafo, fax, redes de computadores etc.

O termo ciberespaço surge no livro de ficção científica intitulado "*Neuromancer*", autoria de William Gibson, no qual atribui-se ao ciberespaço a "concepção de ambiente artificial onde trafegam dados e relações sociais de forma indiscriminada, ou seja, trata-se de um espaço não físico no qual uma alucinação consensual pode ser experimentada a todo momento por seus usuários" (SILVA, 2014).

Para Marietto (2001), o espaço cibernético promoveu mudanças nos conceitos relativos a espaço e tempo, que vão gradativamente sendo adaptados à nova realidade mundial, posto que estão sendo desenhadas estruturas física e de fluxos de informações, representadas pelos *cybermaps*, os quais demonstram: a quantidade de *hosts* em cada unidade espacial; a quantidade de computadores com acesso à *internet;* a quantidade de domínios registrados e a quantidade de usuários de telefone.

Por sua vez, Silva (2014) reporta a definição dada por Manuel Castells (2000) quanto à formação de novas culturas a partir de novos processos de

comunicação, que passam a basear-se, também, no consumo de diferentes sinais, permitindo a mistura do comportamento humano dentro da realidade virtual. Cabe salientar que o ciberespaço se concretiza por meio de uma infraestrutura técnica agigantada, envolvendo a área de telecomunicações e o emaranhado de cabos, fios, redes, computadores etc.

Como amostra do volume e velocidade dos ataques, são indicados aqui dois links que permitem sua visualização em tempo real, são eles: no site da *SonicWall*: https://attackmap.sonicwall.com/live-attack-map/; e uma segunda indicação seria no site do *Fireeye:* https://www.fireeye.com/cyber-map/threat-map.html.

É uma movimentação impressionante.

## O QUE É UM *RANSOMWARE*?

Segundo Oliveira (2018), com a criação e evolução dos diferentes *softwares*, com características específicas, isto é, são amplos e abertos, são criações que permitiram a existência de vulnerabilidades, que em conjunto com eventuais falhas de *hardware*, reúnem brechas para a entrada de ataques aos seus sistemas, conhecidos como ciberataques.

Assim, no que se refere aos crimes cibernéticos, Philot (2021) explica que a internet é uma fronteira ilimitada que reúne indivíduos, empresas e entes governamentais dispostos de forma plana, face ao acesso conquistado a partir de então.

O termo *ransomware* surgiu da fusão entre as palavras *ransom* (resgate) e *malware* (programa malicioso), e tem sido utilizado para explicar uma classe de *malwares* cuja finalidade é bloquear, sequestrar e embaralhar dados pessoais e financeiros existentes nos dispositivos eletrônicos, com a finalidade de extorquir suas vítimas (LEMA e FREITAS, 2021).



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

Com o objetivo de infiltrar-se de forma ilícita em determinado sistema computacional alheio, a infeção de determinado dispositivo por um *ransomware* visa ocasionar danos e bloquear o sistema em questão e todas as informações nele contidas, com a finalidade de pedir resgate monetário por meio de criptomoedas, que é uma moeda virtual não rastreável, já que inexiste qualquer controle estatal.

Segundo Fornasier (2020, p. 209) o r*ansomware* surgiu por volta de 1990, quando Joseph Popp descobriu códigos maliciosos destinados a infectar diferentes computadores. Pimentel (2021) descreve que esses grupos se constituíram na nova indústria do crime.

O sucesso na obtenção dos ataques cibernéticos e consequente recebimento dos resgates permitiram aos criminosos cada vez mais ousadia. Fornasier (2020, p. 209) refere que em 2020, os operadores do *ransomware Doppelpaymer* lançaram um *site* para expor os dados roubados de diferentes empresas que são o foco de seus crimes, cujas vítimas se recusaram a pagar o resgate.

Lema e Freitas (2021, p. 6) explicam que os ataques por meio de *ransomware* afetavam inicialmente a plataforma Windows, mas que sua evolução passou a permitir crimes também sobre outras plataformas, como por exemplo, Apple, Android e Linux. Na atualidade, atingem até mesmo os dispositivos *smartwatches*, por meio do *ransomware Locker.*

Pimentel (2021, p. 3) relata que o conceito inicial sobre um vírus de computador nasceu por volta de 1940, anunciado por John von Neumann em seu artigo *Theory of Self-Reproducing Automata* (“Teoria de autômatos autorreprodutores”), publicado em 1966. Para conceber um vírus de computador eram formulados códigos para danificar as máquinas, os quais deveriam autocopiar-se para infectar novos hospedeiros.

Ainda Pimentel (2021, p. 3) descreve uma breve linha do tempo sobre o surgimento de vírus para computadores:

- 1971 - Vírus *Creeper,* sem objetivo malicioso, foi criado por Bob Thomas, da empresa BBN Technologies, cuja finalidade era autorreplicar-se e ser removido do *host* anterior de forma automática a cada nova infecção (KASPERSKY, 2021, *apud* PIMENTEL, 2021);
- 1982 - Vírus *Elk Cloner*, o primeiro utilizado de forma massiva, atingiu os computadores populares dotados de sistema operacional da Apple II. Depois de 50 inserções do disquete infectado no sistema leitor de um dispositivo, o vírus exibia um poema na tela do aparelho infectado do usuário (AVG, 2021, *apud* PIMENTEL, 2021);
- 1984 - Vírus *Core Wars*, criado nos laboratórios Bell Computers. Era um tipo de vírus mais potente que os anteriores, que comprometia a memória *RAM* das máquinas; alastrou-se nas universidades americanas (MEYER, 2015, *apud* PIMENTEL, 2021);
- 1986 - *Brain* e *Bouncing Ball* foram os *malwares* capazes de infectar o setor de *boot* dos disquetes. Ao mesmo tempo surgiram outros vírus capazes de infectar arquivos com extensão exe e com. O vírus *Brain* é considerado o primeiro vírus capaz de contaminar os *personal computers* (PCs) (MEYER, 2015, *apud* PIMENTEL, 2021);
- Para combatê-lo, John McAfee desenvolveu, em 2012, o famoso antivírus *McAfee*, ao mesmo tempo em que abriu sua empresa homônima (AVG, 2021; OFICINA DA NET, 2015, *apud* PIMENTEL, 2021).
- Já o *Bouncing Ball* é considerado um vírus com função não destrutiva, porém, instalava-se no primeiro setor do disquete, contaminando todo o sistema conforme inseridos outros disquetes (MEYER, 2015, *apud* PIMENTEL, 2021);
- 1989 - Cavalo de troia AIDS (ou PC *Cyborg Trojan*) primeiro *ransomware*, desenvolvido por Joseph Frank Popp. Utilizava-se de um contador para numerar cada reinicialização do sistema operacional, até chegar à 90ª., quando então os arquivos da máquina infectada ficavam ocultos e inacessíveis para a vítima. Uma única chave era utilizada para criptografar e decriptar os arquivos, depois do pagamento do resgate. Uma vez que o criminoso

fornecia uma caixa postal no Panamá para o pagamento de US $189, ele foi descoberto pela polícia, porém, sob a alegação de que seus ganhos seriam destinados às pesquisas pela cura da AIDS, foi considerado legalmente inimputável (PIMENTEL, 2021, p. 3-4);

- 1992 - Vírus Michelangelo, criado para ser inativo e indetectável até o dia 06 de março, aniversário do artista, e a partir dessa data, ele corrompia os arquivos, sobrescrevendo caracteres aleatórios (AVG, 2021, *apud* PIMENTEL, 2021, p. 3-4);
- 1999 - Vírus de *macro* Melissa, criado por David L. Smith, considerado o primeiro a empregar engenharia social para ser espalhado, que ocorre por e-mail, partindo de um dos contatos da vítima (AVG, 2021, *apud* PIMENTEL, 2021, p. 3-4);
- 2000 - Vírus *Iloveyou* infectou milhões de usuários do Windows, incluindo o Pentágono e a CIA. Era difundido por um e-mail com um arquivo anexo denominado *Love-letter-for-you*, que, ao ser executado, retransmitia a mensagem para todos os contatos do usuário (AVG, 2021, *apud* PIMENTEL, 2021, p. 3-4).

Entre 1989 (criação do AIDS) e 2005, foram registrados ataques *ransomware* pouco significativos, readquirindo força apenas em 2005. Durante o período que antecedeu o surgimento do *bitcoin* (em 2007), era possível às investigações rastrearem o pagamento dos resgates; contudo, a partir de 2017, os ataques voltaram com força e frequência bem maiores (PIMENTEL, 2021).

Brito (2016, p. 16) explica a ocorrência de alguns casos entre 2005 e 2006 apontados pela *Trend Micro*, na Rússia, ao verificar uma "compactação de alguns tipos de arquivos e os sobrescrevia com o arquivo compactado com senha". Simultaneamente, era criado um arquivo texto que informava ao usuário o sequestro de seus dados, que poderiam ser liberados para a vítima mediante o pagamento de US$ 300.00.

Com a popularização dessa nova atividade comercial criminosa, a partir de março de 2012 a *Trend Micro* verificou a disseminação de casos pela Europa e América do Norte, quando então, surge um novo tipo de *ransomware* que encriptava

(embaralhava) os arquivos ao mesmo tempo em que bloqueava o sistema operacional do dispositivo atingido (BRITO, 2016, p. 16).

Figura 1 – Representação imagética do bloqueio de informações

*Fonte: UOL (2021).*

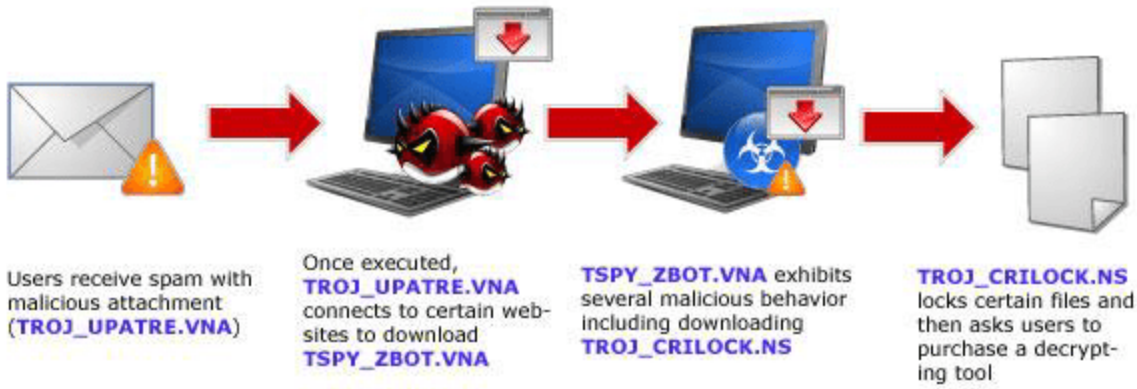
A criptografia visa bloquear o arquivo roubado, induzindo a vítima ao pagamento do resgate. Contudo, cabe destacar que a criptografia também pode ser usada de forma legítima, com a finalidade de "proteger a privacidade e a confidencialidade do usuário" (KOK *et al*., 2019, p. 2). Para tanto, existe uma definição quanto ao limite na frequência da criptografia, que diferencia sua ação legal da ilegítima.

Philot (2021) explica que o termo *malware* abrange categorias diferentes de aplicativos espiões, sendo os *spywares* utilizados para monitorar o comportamento do usuário e roubar seus dados, enquanto os *ransomwares* capturam o sistema, criptografando os arquivos e exigindo o resgate pelos mesmos.

Tais características fizeram com que esses *malwares* fossem denominados *CryptoLocker*, em 2013. Naquele mesmo ano entraram em cena os *crypto-*

*ransomwares* conhecidos como *CryptoDefense* ou *Cryptorbit,* com a finalidade de encriptar “bancos de dados, arquivos *web, office*, vídeos, imagens, *scripts*, textos e outros arquivos do tipo não binário, com posterior deleção dos *backups* existentes” (BRITO, 2016, p. 16).

Figura 2 – Cadeia de infecção do *CryptoLocker*




*Fonte: Brito (2016, p. 17).*

Desde que foi inventado o *ransomware* tem atraído cada vez mais cibercriminosos, devido aos altos índices de retorno e rentabilidade, sendo criadas, gradativamente, versões mais aperfeiçoadas (KOK *et al*., 2019).

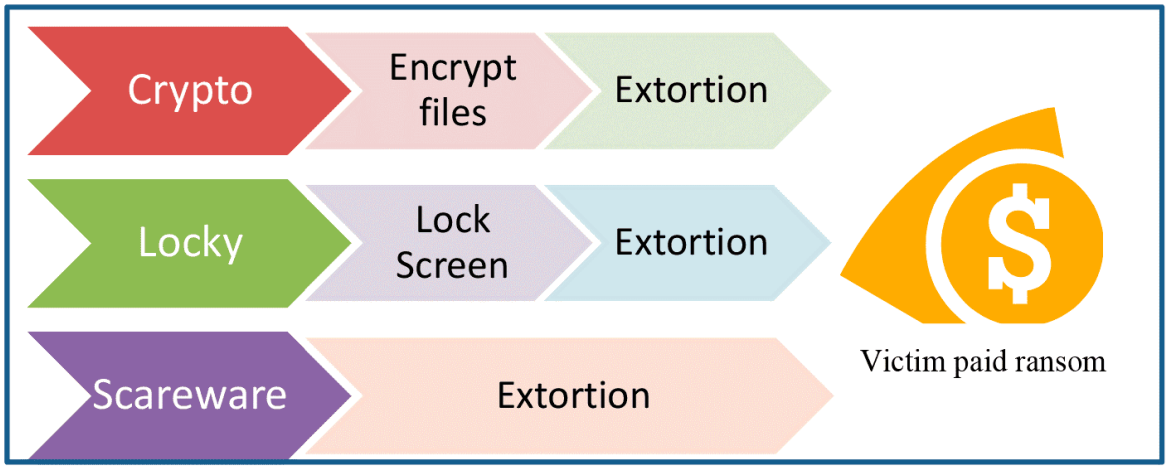
Seu surgimento e expansão foram muito facilitados por meio de um modelo de negócio localizável na *Dark Web*. Trata-se do *Ransomware-as-a-Service* (Raas), conhecido também como *kit ransomware*, cujo funcionamento consiste na venda desse *kit* por um *hacker*, cobrando uma taxa mensal pela venda, ou uma parte do lucro dos golpes, que pode variar de 20% a 50% (GAFETY, 2021).

Lema e Freitas (2021, p. 4) defendem a existência de dois tipos básicos de *ransomware* em circulação, são eles o “*crypto ransomware* e o *locker*

*ransomware*". O *crypto ransomware* é utilizado para embaralhar (encriptar) certos tipos de arquivos de dados e arquivos pessoais, enquanto o *locker ransomware* age bloqueando o computador e impedindo seu uso. Em ambos os casos, os *hackers* tentam obrigar suas vítimas ao pagamento do resgate por meio de canais *online* de pagamento, utilizando-se de chaves para a decriptação.

Já Kok *et al*. (2019) defendem a existência de três tipos de *ransomware,* como demonstra a figura 3.

Figura 3 – Tipos de *ransomware*




*Fonte: Kok et al. (2019, p. 2).*

Segundo Kok *et al*. (2019, p. 2), cada um dos 3 tipos de *ransomware* pode ser assim definido:

1º. tipo - *scareware*. Ele imita uma autoridade que procura alertar sua vítima e pedir o pagamento, sob pena de denúncia legal. Na prática, não representa qualquer perigo real, pois serve apenas para assustar, com a intenção de obter o pagamento do resgate. Na mesma modalidade, existe o *leakware*, usado para ameaçar sua vítima na exposição do delito (não cometido) perante seus amigos e familiares.

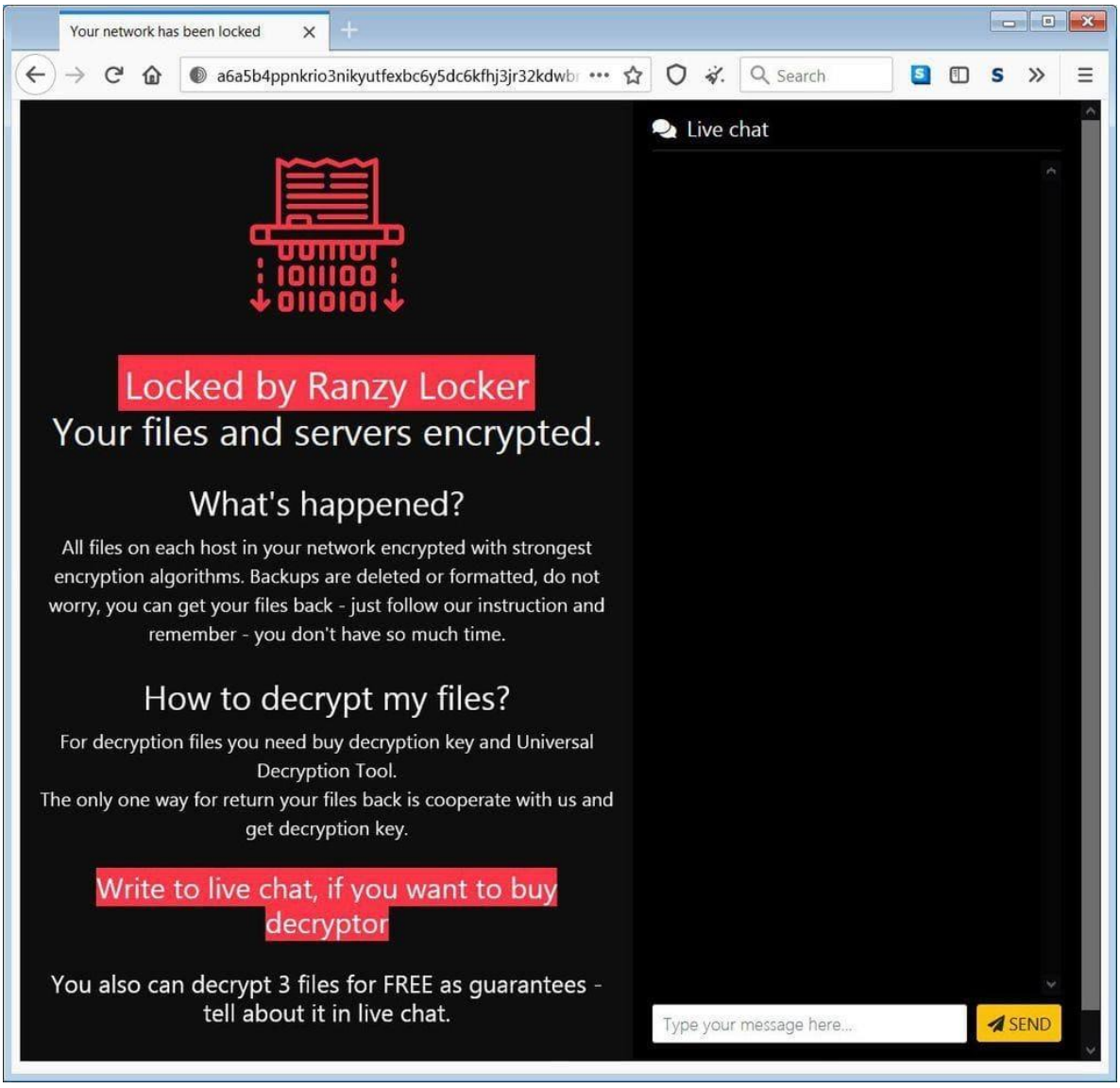
2º. tipo - *locker-ransomware* (ou cacifo-restaurador). *Ransomware* que bloqueia o sistema da vítima quando ela acessa a página de *login.* Considerado por especialistas levemente perigoso, ele pode ser resolvido pela vítima por meio do reinício do sistema, em modo seguro.

3º. tipo - *crypto-ransomware* – trata-se de um *malware* altamente perigoso, uma vez que embaralha os arquivos da vítima, e com isso, impede o acesso aos dados sem sua decriptação.

Ao acessar a rede da vítima, o golpe de *phishing* permite o roubo de documentos antes de realizar sua criptografia, com a finalidade de obter informações e dados de clientes consideradas “sensíveis”, entre elas dados pessoais e registros financeiros, sendo fornecidas pequenas amostras à(s) vítima(s), para que se convença(m) a pagar o resgate, prática considerada “ataque de dupla-extorsão” (BRANCO, 2021).

Ao mesmo tempo que o grupo criminoso fornece à vítima o acesso livre de até três arquivos, comprovando que a restauração acontecerá de fato, esse grupo direciona sua(s) vítima(s) para um *chat* onde pretende realizar a negociação, *chat* instalado no *site* Tor, “onde as comunicações são 100% anônimas” (BRANCO, 2021). A tentativa de convencer a vítima ao pagamento consiste na chantagem sobre a disponibilização pública dos documentos roubados, caso o pagamento não ocorra.

Figura 4 - Imagem do site de pagamento do *Ranzy Locker*




*Fonte: Branco (2021).*

Há outras formas para promover os ataques eletrônicos, ocasionando pânico geral às vítimas, sejam elas pessoas físicas, jurídicas ou instituições governamentais. Uma simples alteração do *Domain Name Service* (DNS), que consiste no desvio do endereço *Internet Protocol* (IP) original, promove o redirecionamento da consulta em andamento para outro IP, que não corresponde aos servidores sob

ataque. Realiza-se um "*defacing* – isto é, uma página que substitui a original pela mensagem do grupo *hacker*" (ALECRIM, 2021A).

Trata-se de um DNS *Spoofing*, ou uma "tapeação de DNS" (ALECRIM, 2021A). Em sendo um golpe mais elementar, ele age da seguinte forma: o usuário digita o endereço do site que pretende acessar, só que, mediante o desvio do DNS, será levado ao DNS do grupo criminoso.

Segundo Carvalho e Pelli (2017, p. 99), em geral, os diferentes dispositivos que se conectam à internet têm o livre acesso aos serviços de DNS para definição de nomes de domínios. Uma vez que inexistem restrições para que pacotes deste tipo de serviço sejam disponibilizados, torna-se de um serviço suscetível aos ataques *ransomware*.

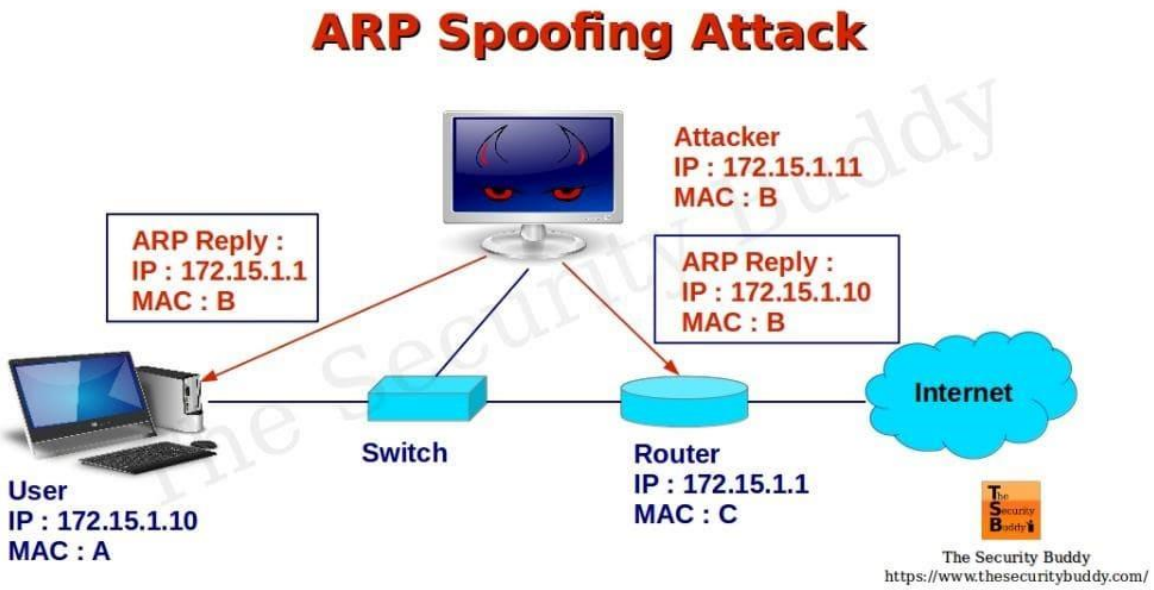
Os ataques ao DNS *Spoofing* são considerados de alta periculosidade, face à falta de estudos e pesquisas para as devidas soluções protetivas Carvalho e Pelli (2017).

Entre as variações quanto ao tipo de ataque, estão: o IP *Spoofing*, é de fácil camuflagem na *internet;* o endereço de IP é falsificado, sugerindo tratar-se de endereço confiável, permitindo ao criminoso obter o acesso não autorizado a determinado dispositivo ou rede; trata-se de um *ransomware* de fácil camuflagem na *internet* (CARVALHO e PELLI, 2017, p. 100).

O DNS *Spoofing* consegue enganar o dispositivo da vítima, redirecionando suas requisições para uma página de interesse do usuário malicioso. Sua ação ocorre em quatro etapas: 1. o usuário alvo realiza uma requisição ao servidor de DNS; 2. o invasor retorna um IP falso para a requisição do usuário alvo antes que chegue à resposta do servidor de DNS com o IP verdadeiro; 3. a resposta do servidor de DNS com o IP verdadeiro é recebida e descartada pelo alvo, pois já foi recebida uma resposta anteriormente; 4. o usuário acessa o endereço fornecido pelo invasor (CARVALHO e PELLI, 2017, p. 100).

Por sua vez, o ARP *Spoofing* promove uma alteração na resposta enviada a um pedido original, remetendo ao usuário uma resposta falsa de *Address Resolution Protocol* (ARP). Com essa resposta falsa, os dados expedidos pelo roteador da vítima serão enviados para o usuário malicioso (CARVALHO e PELLI, 2017).

Figura 5 - Representação imagética de um ARP *Spoofing*




*Fonte: Mitra (2017).*

Se tomado como exemplo o recente ataque ocorrido com o portal do Ministério da Saúde brasileiro, noticiado como *ransomware*, mas analisado pelo grupo *Anonymous*, em sua colaboração com explicações e gráficos, verificou-se que de fato, o que ocorreu foi um redirecionamento do DNS daquele MS, comprovado com uma explicação básica dada pelo grupo *Anonymous* (MARTON, 2021).

Tal análise consistiu na observação de uma pista falsa dada pelos criminosos, quando informaram terem baixado 50 tb (*terabytes*) de dados daquele Ministério, cujo IP está hospedado no Japão. Trata-se de uma transferência considerada impossível de ser realizada em servidores de alto tráfego em curto espaço de

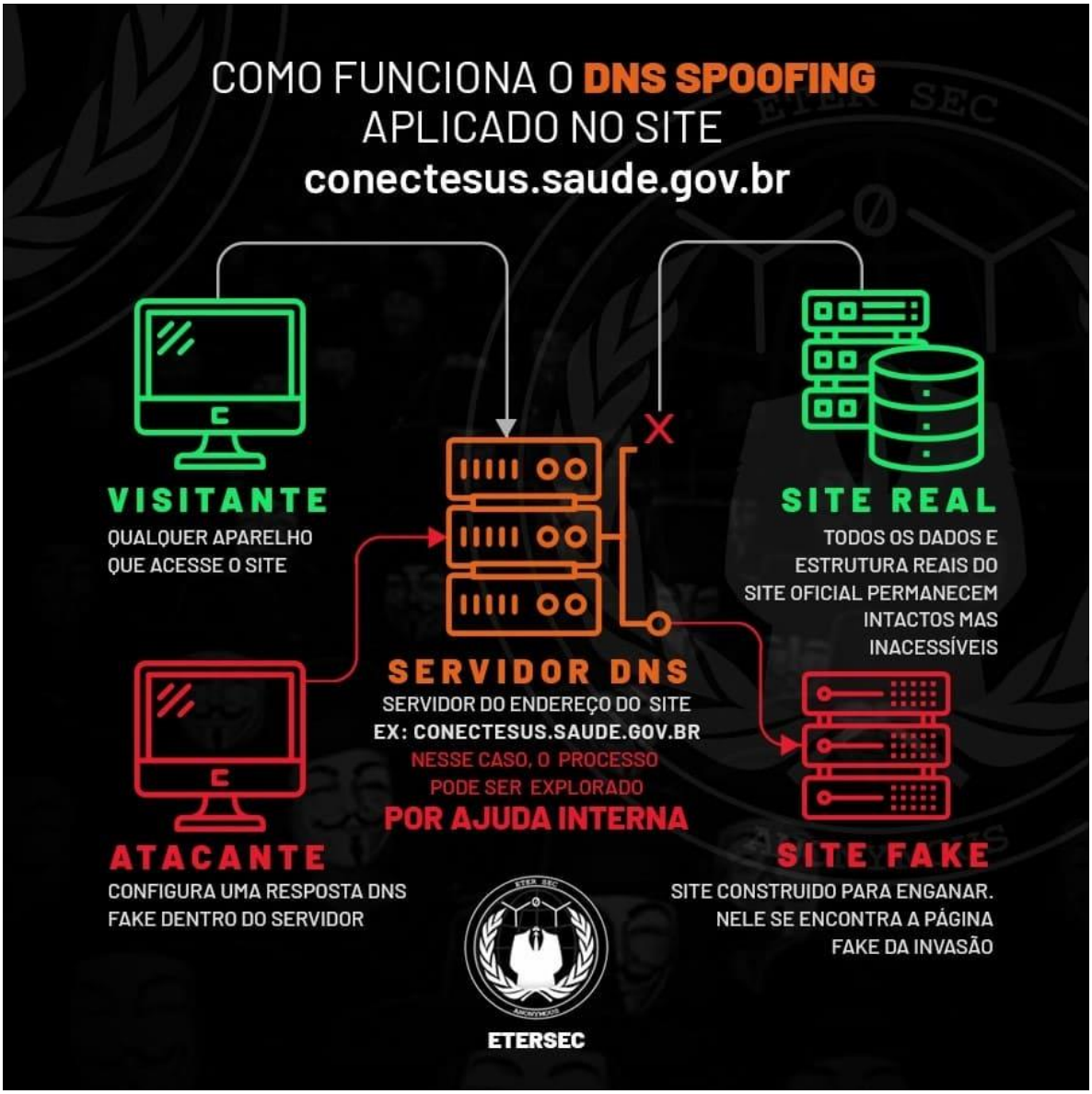


RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

tempo, além de não terem sido dadas amostras de informações recentes (ALECRIM, 2021A).

O desvio do DNS nesse caso foi demonstrado pelo grupo *Anonymous*, como demonstra o gráfico 1.

Gráfico 1 – Desvio de DNS




*Fonte: Alecrim (2021A).*



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

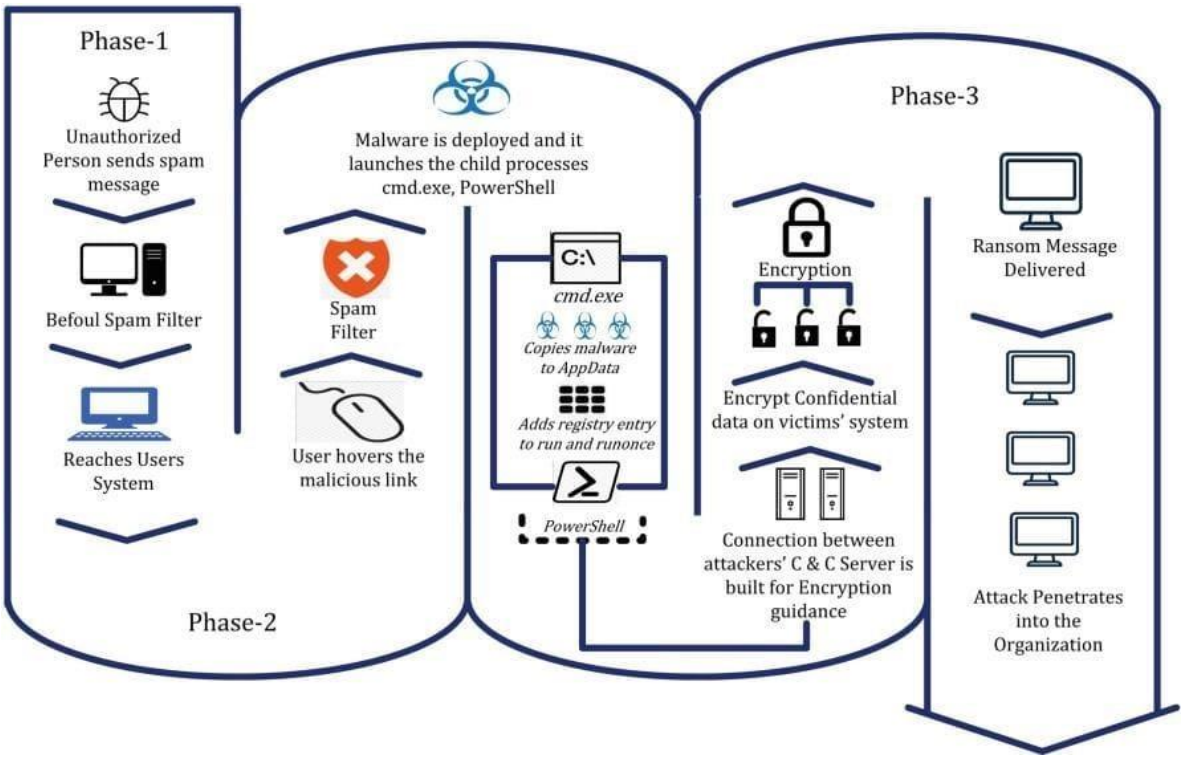
A solução encontrada pelos criminosos foi remover o *defacer*, pois não teria como restaurar os dados, porque não teriam sido roubados.

## ÓRGÃOS DE SEGURANÇA ELETRÔNICA NORTE-AMERICANOS

Dados e informações pessoais e financeiras de um indivíduo/empresa/instituição constituem-se em elementos fundamentais a serem protegidos. Essa proteção implica “na confidencialidade, integridade e disponibilidade, que constituem os três pilares da segurança da informação” (PHILOT, 2021, p. 9).

A confidencialidade envolve a privacidade sobre informações sensíveis, já que se refere à necessidade de quaisquer dados estarem fora do alcance de pessoas desautorizadas; além disso, todas as informações devem permanecer intactas.

Figura 6 – Representação imagética de um ataque de resgate




*Fonte: Kumari et al. (2019, p. 18).*



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

A Agência de Cibersegurança e Segurança de Infraestrutura dos Estados Unidos (CISA) atua em conjunto com o *Federal Bureau of Investigation* (FBI), quanto à ocorrência de crimes eletrônicos nos Estados Unidos (BRANCO, 2021). Em outubro de 2021 o FBI alertou o governo norte-americano sobre a ocorrência de ao menos 30 ataques naquele ano, realizados contra empresas locais das áreas de tecnologia, transporte e informação. Além de monitorar as ocorrências, CISA e FBI indicam também as formas de identificação de tentativas desse tipo de ameaça.

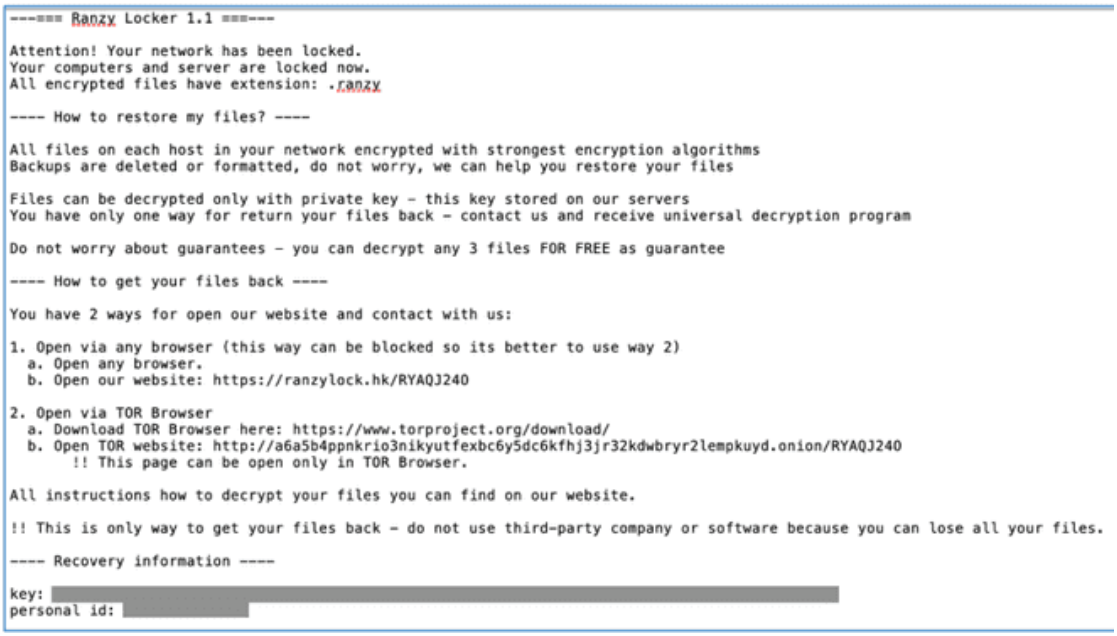
Segundo o FBI, entre os grupos envolvidos está o *Ranzy Locker*, cujo aviso de sequestro assemelha-se com golpes realizados por dois outros grupos *ransomware ALO* e *ThunderX*, aparentemente sumidos, que, possivelmente, reuniram-se para operar como *Ranzy Locker* (BRANCO, 2021).

A invasão aos diferentes sistemas consiste em ataques de força-bruta ou golpes de *phishing*, por meio dos quais os criminosos tentam utilizar credenciais aleatórias até obterem o acesso, ou pela avaliação das vulnerabilidades para o roubo de senhas de e-mails do Microsoft *Exchange*, programa que permite o acesso aos e-mails dos usuários mesmo se desconectados da *internet* (BRANCO, 2021).



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

Figura 7 - Mensagem de aviso do sequestro do *Ranzy Locker*




*Fonte: Branco (2021).*

No que se refere à legislação norte-americana, uma vez que diferentes leis norte-americanas são estaduais. Masseno e Wendt (2017) referem que a seção 523 do Código Penal da Califórnia prevê a qualificação do crime de extorsão, onde está assegurada a liberdade da vida em dispor de seu patrimônio, relativamente aos seus dispositivos, como de suas informações confidenciais.

Contudo, em março de 2022, foi aprovada pelo senado norte-americano uma nova lei relativa à defesa de empresas e instituições que sofram qualquer ataque cibernético. Trata-se de um esforço conjunto entre republicanos e democratas, visando a proteção das áreas de infraestrutura críticas, assim como da economia da nação (TIC NEWS, 2022).

É considerada "uma legislação bipartidária, de senso comum, que vai ajudar a proteger as infraestruturas críticas de ciberataques implacáveis que ameaçam tanto a nossa economia como a nossa segurança nacional", segundo Gary Peters, da comissão de segurança nacional do senado (TIC NEWS, 2022).

A partir da nova lei, todas as operações de infraestruturas críticas obrigam-se a alertar o Departamento de Segurança Nacional em até 72 horas da ocorrência de qualquer ataque sofrido, além de informar em até 24 horas caso tenha efetuado o pagamento de resgate para acessar novamente os dados roubados (TIC NEWS, 2022).

## RECENTES ATAQUES CIBERNÉTICOS OCORRIDOS NOS ESTADOS UNIDOS

Empresas de porte e sistemas governamentais norte-americanos têm sido os alvos mais frequentes de ataques *hackers*, que usam *malwares* capazes de bloquear os sistemas ao ponto de pedirem quantias altas para o resgate de dados. Medeiros *et al*. (2020) referem recorrentes ações criminosas para bloquear, roubar e pedir resgates pagáveis por meio de criptomoedas, as quais não podem ser rastreadas.

Medeiros *et al*. (2020, p. 653) informam que há uma preferência dos criminosos cibernéticos por "*sites* públicos, que operam na criação de clones simulando os endereços de *sites* oficiais". Estes autores referem vários ataques *hackers* ocorridos contra instituições norte-americanas, as consequências e soluções adotadas naquele momento.

No que se refere à forma como ocorre a invasão de um sistema empresarial pelo *ransomware*, a *Sophos*, empresa inglesa desenvolvedora e fornecedora de softwares e *hardwares* de segurança, incluindo antivírus, *antispyware, antispam*, controle de acesso de rede, *software* de criptografia e prevenção de perda de dados para *desktops*, servidores para proteção de sistemas de e-mail e filtragem para *gateways* da rede, tabulou as formas e porcentagens da incidência das invasões cibernéticas, como demonstra na tabela 1.



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

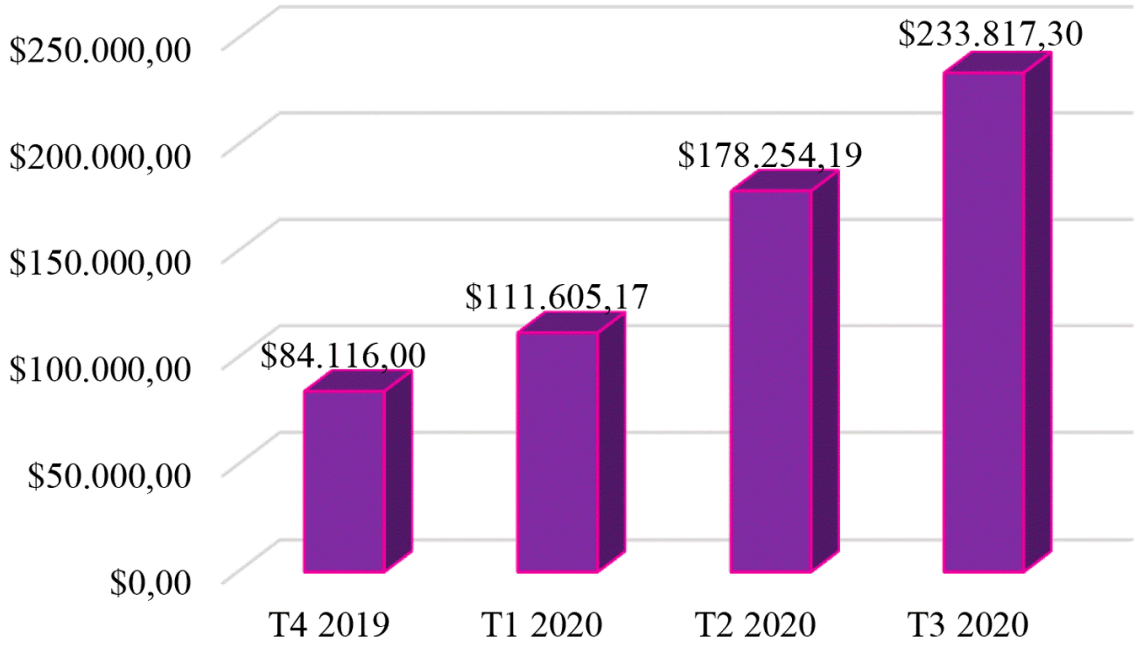
Tabela 1 – Formas de entrada do *ransomware* em %

| COMO O *RANSOMWARE* ENTRA NO SISTEMA DA ORGANIZAÇÃO | % INCIDENTES |
|---|---|
| **Via *download* de arquivo / e-mail com *link* malicioso** | 29% |
| **Via ataque remoto no servidor** | 21% |
| **Por e-mail com anexo malicioso** | 16% |
| **Instâncias na Nuvem pública configuradas incorretamente** | 9% |
| **Por meio de nosso protocolo de área de trabalho remota (RDP)** | 9% |
| **Por meio de um fornecedor que trabalha com nossa organização** | 9% |
| **Por meio de um dispositivo USB /mídia removível** | 7% |

*Fonte: Pereira e Neves (2021, p. 75).*

Por sua vez, os dados tabulados em 2020 pela Coveware, empresa especializada em segurança cibernética e proteção e recuperação de golpes eletrônicos, é alto o volume de pagamento de resgates de *ransomware* por parte das grandes organizações norte-americanas, ocasionando a projeção para cima nos valores sugeridos nas ações sequentes desses grupos criminosos (PEREIRA e NEVES, 2021). O gráfico 2 demonstra o aumento dos pagamentos de resgates em 31%, chegando ao montante de US$ 233.817.

Gráfico 2 – Média trimestral de pagamento de resgate de *Ransomware*



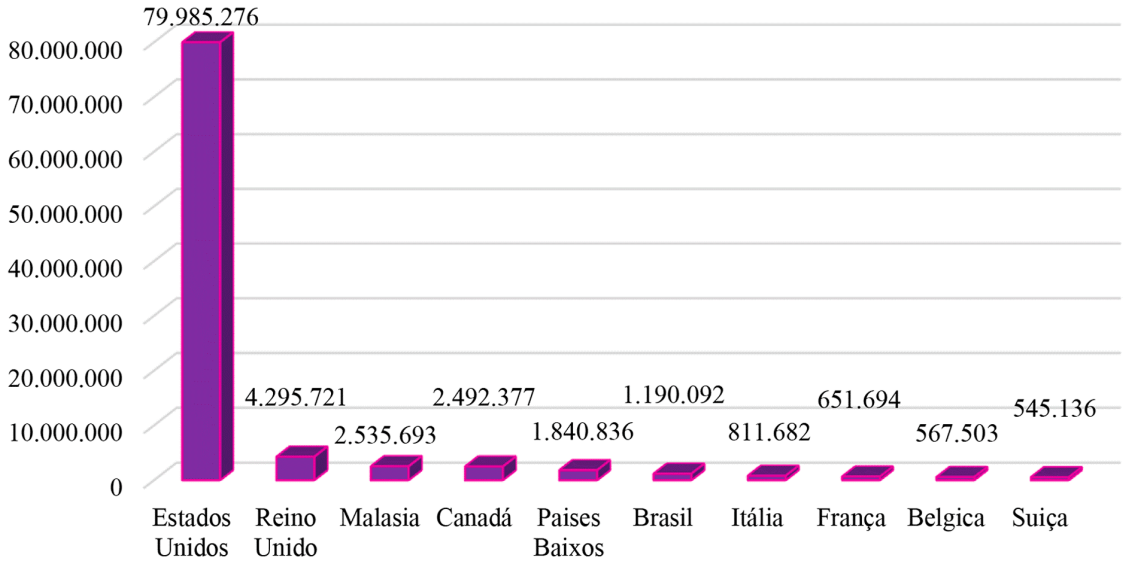

*Fonte: Pereira e Neves (2021, p. 73).*

Já a *SonicWall*, empresa especializada na criação dimensionamento e gerenciamento de segurança em ambientes em nuvem, híbridos e tradicionais, elaborou um relatório relativo às ameaças cibernéticas ocorridas até julho de 2020 ocorridas em diferentes países, como demonstra o gráfico 3 (PEREIRA e NEVES, 2021).



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

Gráfico 3 – Ataques *ransomware* ocorridos em 10 países até julho de 2020




*Fonte: Pereira e Neves (2021, p. 74).*

Com o objetivo de apresentar os casos ocorridos nos últimos anos nos Estados Unidos, os principais ataques cibernéticos a empresas e instituições passam a ser aqui relatados.

Em maio de 2017, ocorreu o ataque do *ransomware WannaCry*, considerado o maior de todos os tempos, afetando computadores em diferentes partes do mundo. Esse *malware* teve como alvo o sistema da Microsoft Windows instalado em diferentes tipos de dispositivos. Medeiros *et al*. (2020) explicam que foi o cibercrime que ocasionou bilhões de dólares em prejuízos financeiros, passando a ser considerado, a partir de então, a grande lição ao que ficou denominado como “alfabetização digital”, no sentido da adoção de *backups* sistemáticos.

O *ransomware WannaCry* foi considerado um *malware* que ocasionou uma verdadeira “epidemia global que aconteceu em maio de 2017, espalhando-se por computadores que detivessem a instalação do Microsoft Windows”, a serem liberados somente mediante o pagamento de resgate em *bitcoins*. Este ataque cibernético foi possível, em parte, devido à falta de hábito na atualização dos

softwares instalados nos milhares de computadores usuários do referido sistema (KASPERSKY LAB, 2022A).

Kumari *et al*. (2019) referem que o *ransomware WannaCRy* afetou dispositivos em grande escala, atingindo máquinas em 150 países em menos de 24 horas, tendo por alvo os sistemas operacionais Windows da Microsoft. O resgate variou de US$ 300 a US$ 600, a serem pagos por *bitcoins*. Com o avanço dos ataques e obtenção do pagamento dos resgates, essa quantia chegou a US$ 1.077, conforme Relatório Symantec de 2017.

Entre as vítimas desse *malware*, estão o Serviço Nacional de Saúde Britânico, o expedidor internacional FedEx, a Telefônica, entre outras empresas de grande porte. Além destas, os sistemas de departamento de polícia na Índia e diversas empresas locais foram prejudicadas. Já os países atingidos pelo *WannaCry*, podem ser mencionados a Espanha, Portugal, Rússia, Ucrânia, e Taiwan (KUMARI *et al*., 2019).

Face à gravidade desse crime e da publicidade alcançada por essa contaminação, foram iniciadas algumas investigações. Um boletim de segurança emitido pelo Laboratório Kaspersky assegurou que, em 2016, aproximadamente 20 empresas pagaram o resgate, sem jamais receberem seus documentos de volta. Por sua vez, a IBM descobriu que 70% dos administradores por ela investigados informaram que teriam pago os resgates, enquanto a *Osterman Research* informou que o total de pagantes de resgate foi mínimo (KUMARI *et al*., 2019).

A grande questão que permitiu todos esses crimes cibernéticos deve-se à projeção do *bitcoin* que, em sendo uma moeda indetectável, proporcionou cada vez mais ousadia a esses grupos criminosos (KUMARI *et al*., 2019).

Em março de 2020, o centro de testes do novo coronavírus existente no Hospital Universitário de Brno, na República Tcheca, foi alvo de um *ransomware*. “Criminosos conseguiram acesso ao sistema do hospital e criptografaram os

bancos de dados (NEWMAN, 2020; ARBULU, 2020, apud MEDEIROS *et al*., 2020, p. 653).

Uma vez que a direção do referido hospital decidiu enfrentar o crime recusando-se a efetuar o pagamento de resgate, adotou-se como solução a suspensão momentaneamente dos atendimentos, por meio do remanejamento de seus pacientes para outros serviços médicos (MEDEIROS *et al*., 2020).

Ainda em março de 2020 o sistema do Distrito de Saúde Pública de Champaign-Urbana (Illinois) também foi alvo de um *ransomware*, prejudicando aquele serviço médico. Uma vez que detinha *backup* atualizado de seus dados eletrônicos, foi possível a este serviço de saúde deliberar sobre a recusa ao pagamento de qualquer resgate, sendo que seus dados foram apenas levemente afetados pela ação dos criminosos (MEDEIROS *et al*., 2020, p. 653).

Em 07 de maio de 2021 foi feito um ataque cibernético contra a empresa Colonial Pipeline, empresa do ramo petroleiro responsável pelo fornecimento de aproximados 2,5 milhões de barris de óleo que circulam diariamente pelos dutos daquela organização, que é a responsável pelo fornecimento de 45% de diesel e gasolina para toda a costa leste dos Estados Unidos (ALECRIM, 2021B).

Como resultado, surgiram as longas filas nos postos de combustíveis, o aumento de preços e a paralisação parcial ou total dos serviços. O fornecimento de combustíveis foi interrompido por alguns dias, levando o governo norte-americano a decretar estado de emergência daquela região já em 09 de maio (ALECRIM, 2021B).

Mediante a invasão cibernética, a direção da empresa ordenou o desligamento de grande parte de seus sistemas, na tentativa de conter o crescimento daquele ataque. Para conter a dimensão da situação, e, face à pressão sofrida para a normalização do abastecimento, a Colonial Pipeline decidiu pagar o montante exigido, fixado em 75 *bitcoins* pela *Dark Side*, valor que correspondia, à época, a

US$ 5 milhões. Essa decisão permitiu a normalização dos sistemas eletrônicos da empresa em poucos dias (ALECRIM, 2021B).

As investigações promovidas pelo FBI permitiram que fosse recuperada boa parte do resgate pago ainda em junho daquele ano. Além disso, permitiram a descoberta de pistas sobre outros ataques cibernéticos ocorridos no primeiro trimestre de 2021, que atingiram inúmeras outras empresas, cujos resultados podem ter alcançado a marca dos US$ 50 milhões (ALECRIM, 2021B).

Por esses motivos, o governo norte-americano divulgou a oferta de uma recompensa da ordem de US$ 10 milhões para grupos especializados que pudessem colaborar com informações sobre os membros do *DarkSide*, que aparentemente, encerrou suas atividades. Especula-se que seus integrantes podem ter fundado um novo grupo intitulado *BlackMatter* (ALECRIM, 2021B).

No final de maio de 2021 a multinacional JBS, que opera no processamento de carnes bovina, suína, ovina e de frango, e no processamento de couros, sofreu ataque cibernético em seus servidores dos Estados Unidos e Austrália, decidindo, ao final, pelo pagamento de um resgate total de US$ 11 milhões (LAVADO, 2021).

Depois de pagar o resgate, a companhia tornou pública a informação sobre os servidores de *backup* da companhia não terem sido afetados, divulgando ainda a tomada de "medidas imediatas, suspendendo todos os sistemas afetados, notificando as autoridades e ativando a rede global da empresa de profissionais de TI e especialistas terceirizados para resolver a situação". Por fim, explicou ainda que a decisão pelo pagamento do resgate deveu-se ao possível atraso em "certas transações com clientes e fornecedores" (LAVADO, 2021).

Em outubro de 2021 foi cometido um ataque *hacker* DDoS (*Distributed Deny of Service*) contra o *United States Department of Health and Human Services* (HHS), que é o Departamento de Saúde e Serviços Humanos dos EUA. A invasão ao sistema de saúde no sudeste da Flórida teve acesso aproximadamente a 1,3

milhão de pessoas, compreendendo dados como numeração de identidade, histórico médico de pacientes e dados bancários, expostos na invasão da Broward *Health,* que é uma rede que compreende mais de 30 unidades e atende por volta de 2 milhões de pacientes em Broward, na Flórida (LYNGAAS, 2022)

O ataque ao DDoS, também conhecido como ataque de negação de serviços distribuído, consiste em enviar inúmeras solicitações de acesso até esgotar o limite da capacidade específica aplicável a todos os recursos de rede, entre eles, a infraestrutura que permite o funcionamento adequado do site de determinada organização/instituição. Dito de outra forma, para promover o envio exagerado de solicitações a um site, o criminoso estabelece uma rede zumbi de computadores infectados, controlando todas as ações de cada máquina para promover a sobrecarga (KASPERSKY, 2022B).

Figura 8 - Representação imagética de um ataque DDoS

*Fonte: Kaspersky (2002B).*



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

Como resultado da divulgação desse fato, o referido cibercrime levou os usuários do sistema de saúde norte-americano a procurarem informações seguras sobre a pandemia da Covid 19 em outras fontes, evitando a consulta ao site oficial daquele órgão, por temerem o roubo de seus dados (MEDEIROS *et al*., 2020).

Em dezembro de 2021, um segundo caso refere-se ao Lincoln College, fundado em 1865. Foi uma universidade que promoveu grandes feitos no país, entre eles a constituição norte-americana, a conquista de direitos civis individuais, além de gerar oportunidades profissionais no meio rural no estado de Illinois (PRIVACY TOOLS, 2022).

Segundo a revista *PPlware* (2022), especializada em notícias e informações da área tecnológica, o Lincoln College é uma "instituição que ultrapassou períodos muito difíceis ao nível económico e social que foram transversais a todo o mundo, como as duas Guerras Mundiais, a Gripe Espanhola ou a Grande Depressão, mas não foi capaz de suportar um ataque informático de *Ransomware*, depois de dois anos de pandemia".

Apesar dos avanços digitais conquistados para seu sistema operacional, o Lincoln College falhou no quesito investimentos em segurança cibernética. Com isso, para além do drama da Covid 19, em dezembro de 2021 foi vítima de determinado tipo de *ransomware* utilizado para invadir seus sistemas, que, tendo seus servidores e dados bloqueados, ficando impedidos de identificar aproximadamente 600 estudantes que iriam efetivar suas matrículas, assim como as doações (PRIVACY TOOLS, 2022).

Mesmo com investimentos da ordem de “US$ 100.000 para revitalizar os bancos de dados e barrar mais ataques, o recurso utilizado não havia sido um *malware* comum e sim um *software* potencialmente destrutivo”, foram necessários apenas quatro meses para o fechamento daquela instituição, depois de 157 anos de atividades (PRIVACY TOOLS, 2022).



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

Em janeiro de 2022 foi a vez do Centro de Detenção de Bernalillo, condado mais populoso do novo México. Realizou-se uma invasão cibernética que deixou fora do ar, entre 00h e 5h da manhã, todas as câmeras de segurança e mecanismos de abertura e fechamento das portas, ficando desativadas. Além disso, todos os dados contendo as informações pessoais completas dos detentos e crimes cometidos ficaram indisponíveis (TECMUNDO, 2022).

Figura 9 - Centro de Detenção de Bernalillo (Novo México)


*Fonte: Tecmundo (2022).*

Até que a solução técnica fosse efetivada, as visitas foram suspensas, os detentos foram mantidos em suas celas, sendo necessário o uso de chaves manuais para abrir ou fechar as portas necessárias.

Por sua vez, estão os crimes cibernéticos aos aplicativos de videoconferência. É unânime a ideia sobre o fato de que nenhum aplicativo de comunicação é 100% seguro quanto ao sigilo das informações que abrigam, incluindo os arquivos em nuvens, já que as nuvens são servidores físicos localizados em diferentes países, como demonstrou o caso Snowden, por exemplo (MEDEIROS *et al*., 2020, p.655).

Outra vulnerabilidade dos aplicativos de videochamadas consiste na possibilidade dos cibercriminosos ouvirem as comunicações que ocorrem no decorrer de

determinada conferência, criando situações de constrangimento, ao tentarem encerrar a reunião ou sala de aula, por exemplo, ou ainda transmitindo mensagens racistas e/ou pornográficas. Entre as diferentes ocasiões, pode-se mencionar a exposição de “fotos de reuniões em redes sociais, exibindo o código de identificação da chamada, como fez o Primeiro-Ministro britânico, Boris Johnson, no final do mês de março” (MEDEIROS *et al*., 2020, p. 655).

## MELHORIAS NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

De acordo com o portal Tecmundo (2022), os ataques de *ransomware* são considerados como “as maiores ameaças cibernéticas para empresas privadas e instituições públicas nos EUA”. Tal afirmação deu-se quando o Tecmundo reportou dados computados pela Forcepoint, multinacional americana desenvolvedora de *softwares* de segurança para computadores, proteção de dados, corretor de segurança de acesso à nuvem, *firewall* e soluções de domínio cruzado.

Tal pesquisa realizada pela Forcepoint tabulou números quanto à crença de 75% dos profissionais especializados em segurança vislumbravam o crescimento de novos ataques de *malware* e *ransomware* às organizações nos próximos 12 meses. Segundo relatório do Tesouro norte-americano sobre um possível recorde de pagamento de *ransomware* naquele ano, foi criada uma força-tarefa no país para combater esses crimes em 2021 (TECMUNDO, 2022).

Por sua vez, a CISA divulgou uma lista das más práticas eletrônicas, são elas: uso da autenticação de fator único; uso de *software* sem suporte (ou em fim de vida); uso de senhas e credenciais conhecidas/fixas/padrão (OWAIDA, 2021).

Entre as várias possibilidades de proteção efetiva de seus sistemas operacionais, seguem-se indicações reunidas de diferentes fontes.



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

Brito (2016, p.12) refere a importância da Gestão da Segurança da Informação. Explica que empresas e instituições estão sempre em busca de soluções para mitigação dos crimes cibernéticos, atividade em ascensão. Trata-se de identificar e implementar boas práticas que visam a proteção eficaz de dados e sistemas empresariais e governamentais, por meio de políticas públicas, contando ainda com a definição de funções e responsabilidades específicas.

Owaida (2021) reporta as recomendações desenvolvidas pela CISA, sobre as empresas adotarem a Autenticação Multifator (MFA) como opção mais segura, pois confere “uma camada extra de segurança e faz com que seja excessivamente difícil a realização de ataques a contas de usuários”. Este autor refere que resultados satisfatórios obtidos pelo uso do MFA, relatados em estudo elaborado pelo Google, em parceria com a Universidade de Nova York e Universidade da Califórnia.

Segundo a Cisa, tal estudo demonstrou que o “uso da MFA resultou no bloqueio de 100% dos *bots* automatizados, 99% dos ataques de *phishing* em massa e 66% dos ataques direcionados às contas de usuários do Google” (OWAIDA, 2021).

Entre os diferentes sistemas multicamadas, Kok *et al*. (2019, p.3) referem o *RansomWall*, cuja última camada usa “o *Machine Learning* para prever o resultado de recursos coletados na análise estática, análise dinâmica e camadas armadilhadas”. É considerado um método com alto índice de detecção, cuja “taxa chega a 98,25% é quase zero falsos positivos usando um algoritmo de *Gradient Tree Boosting*”.

Há ainda o *AntiBiotics*, que é baseado em autenticação e aplicativos, sendo usado para controlar o acesso aos diferentes arquivos em determinado equipamento. É considerado eficaz, uma vez que a negação de acesso aos arquivos pode impedir o *ransomware* de capturar o arquivo (KOK *et al*., 2019, p.3).



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

No que se refere às buscas por anomalias no sistema, tem-se que os processos de monitoramento e diretórios de arquivos específicos devem incluir um processador, o uso de memória e taxas de E/S, cujas operações são realizadas por vários dispositivos externos, permitindo a transferência de dados entre o ambiente externo e o computador. No momento em que alguma anomalia for detectada, surge para o usuário "uma mensagem para remover o suspeito de resgate" (KOK *et al*., 2019, p.3).

Podem ainda serem criadas armadilhas denominadas *honeyfile*, que tem duas funções: atrair o ataque para um arquivo que não é o real, e a segunda, analisar o tipo de ataque, permitindo com isso, a melhor compreensão das ameaças existentes, e a elaboração de um plano para a eliminação de novas ameaças (KOK *et al*., 2019).

Kumari *et al*. (2019) explicam que é possível quebrar a simetria entre a visão de um analista antivírus e as ideias e processos de ação dos criminosos. Trata-se do uso do conceito de chave pública da criptografia. Enquanto o analista antivírus está atento a uma chave pública existente em determinado *software* malicioso, o criminoso vê a chave pública e também a chave privada correspondente, que está fora do *malware,* já que esse atacante foi o criador dos pares de chaves.

Ainda Kumari *et al*. (2019) refere que pessoas físicas, empresas de diferentes ramos ou instituições governamentais podem ser alvo de de diferentes tipos de ataques cibernéticos, existindo ainda uma lista com os diferentes tipos de resgates: *CryptoLocker*, *CryptoLocker.F* e *TorrentLocker*, *CryptoWall*, *Fusob*, *WannaCry*, *Petya*, *Bad Rabbit* e *SamSam*.

Entre as diferentes abordagens para viabilizar a análise dos vários tipos de *malweare*, como por exemplo, o uso do método *Randep* para mapear o comportamento de um *malware*. Cada ataque *ransomware* consiste em três fases, são elas: "na primeira fase ocorrem operações furtivas, na segunda ocorrem



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

atividades suspeitas, e na terceira são feitas as ações óbvias" (KOK *et al*., 2019, p.3).

A análise de um *ransomware* deve ser feita por meio de duas abordagens: "a análise estática, que verifica o código fonte do *malware*, e a análise dinâmica, que verifica as ações do *malware* após sua execução" (KOK *et al*., 2019, p.3). Já o método *RanDroid* tem o objetivo de identificar ameaças em forma de texto ou imagem, a partir de algum código de aplicação.

No que se refere aos ataques *Spoofing,* por meio do estudo elaborado por Carvalho e Pelli (2017, p.99), constatou-se que a aplicação das técnicas de seleção de características e classificação de padrões para detecção de DNS *Spoofing* em redes locais de computadores, foram verificados resultados altamente positivos, "cuja média foi de 98,33% ± 0,64% na detecção na classe de falha da rede, ou seja, quando essas estavam sob ataque de DNS *Spoofing".*

Por sua vez, Branco (2021) reporta o manual de instruções publicado pela CISA, sugerindo boas práticas protetivas, que colaborem para impedir novos crimes virtuais:

1. Fazer *backups* de dados frequentes, mantendo-os em um ambiente *offline* protegido por criptografia;
2. Criar um plano básico de cibersegurança para responder a incidentes, manter operações e se comunicar sobre as etapas que devem ser seguidas;
3. Usar configurações adequadas de acesso remoto, conduzir análises frequentes em busca de vulnerabilidades e manter *softwares* atualizados;
4. Assegurar que todos usam configurações de segurança recomendadas, desabilitando portas que não são usadas e protocolos como o *Server Message Block* (SMB) quando isso for possível;



RC: 124626
Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware

5. Práticas boas práticas de higiene cibernética: manter *softwares,* antivírus e *antimalware* ativos e atualizados, limitar o uso de contas com acesso privilegiado e usar sempre soluções de acesso multifator quando possível.

Segundo Brito (2016, p. 12-13), foram desenvolvidas algumas normas de padrão internacional para a elaboração e manutenção dos processos relativos à Gestão da Segurança da Informação, que ficaram conhecidas como série 27000. Para tanto, foram elencadas 10 premissas básicas aplicáveis às diferentes organizações, são elas: Política de Segurança da Informação; Segurança Organizacional; Classificação e controle dos ativos de informação; Segurança em pessoas; Segurança Física e Ambiental; Gerenciamento das operações e comunicações; Controle de Acesso; Desenvolvimento de Sistemas e Manutenção; Gestão da continuidade do negócio e a Conformidade.

A ISO 27001 pertence à séria mencionada. Trata-se da norma internacional que especifica o Sistema de Gestão de Segurança da Informação (SGSI), cujo objetivo é a adoção de um conjunto de requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o SGSI, de modo a implementar controles que visem gerir adequadamente os riscos de Segurança da Informação presentes nas organizações (BRITO, 2016).

Além disso, a referida ISO 27001 tem a finalidade de assegurar que todos os dispositivos sejam mantidos com a segurança virtual adequada, sendo necessária a atualização permanente do sistema operacional, prevenindo-se de novas ameaças, vulnerabilidades e impactos comerciais negativos (BRITO, 2016). Tal norma abrange empresas relacionadas à indústria, comércio, serviços, instituições governamentais e às não governamentais.

Entre os avanços obtidos para reforçar as boas práticas na Gestão em Segurança da Informação, Kumari *et al*. (2019) destacam o antibiótico, enquanto mecanismo para proteção de *ransomware*, cuja abordagem consiste em vários tipos de

autenticação periódica, como a biométrica e humana, que se dá por meio do *CAPTCHA*. O conceito básico do antibiótico é a adaptação à necessidade de respostas na autenticação do usuário, mantendo os níveis de segurança projetados.

## CONCLUSÃO

A velocidade com que os recursos eletrônicos e diferentes tecnologias avançaram ao longo do tempo permitiram que a humanidade vivenciasse, no presente, situações positivas altamente arrojadas, exemplificadas nas muitas possibilidades ocasionadas pela globalização, diante da qual os indivíduos se comunicam-se e constroem seus saberes e recebem informações e notícias em tempo real.

Em resposta à questão norteadora relativa ao tema presente, tendo como pergunta “quais seriam as boas práticas em Gestão de Sistemas em Tecnologia da Informação e como podem colaborar para mitigar os ataques *ransomware*?”, tem-se que para além da análise da literatura selecionada quanto às teorias, aos eventos relatados e de toda a evolução que vivemos, o trabalho dos especialistas deve anteceder as ações de criminosos, por meio da inteligência artificial, pelas técnicas de prevenção existentes, e do desenvolvimento de instrumentos voltados à segurança e proteção de dados pessoais e financeiros tanto de pessoas físicas quanto das organizacionais, antevendo os próximos passos dos grupos criminosos que emergem da *dark web*.

Entre as várias propostas de prevenção listadas neste artigo, já adotadas pelos especialistas dentro das organizações, acredito sinceramente na necessidade da conscientização, educação e treinamento em Segurança da Informação, por meio da adoção das boas práticas descritas pela Norma ISO/IEC 27001.

Com essa ação as empresas poderão colocar em prática uma boa gestão em Tecnologia da Informação, prevenindo-se ante os erros mais simples, como

exemplo o uso de senhas fracas, que seus colaboradores venham a clicar em qualquer *link* recebido de e-mails desconhecidos, ou ainda clicar em qualquer anúncio que aparecer em um determinado site da *internet.*

## REFERÊNCIAS

ALECRIM, Emerson. **PF diz que dados do Ministério da Saúde não foram criptografados por hackers.** 10 dez 2021A. Disponível em:

https://tecnoblog.net/noticias/2021/12/10/pf-diz-que-dados-do-ministerio-da-saude-nao-foram-criptografados-por-hackers/; acesso em 06 jul 2022.

ALECRIM, Emerson. **EUA pagam US$ 10 mi por hackers do ransomware que atacou Colonial Pipeline**. Matéria publicada em nov 2021B. Disponível em: https://tecnoblog.net/noticias/2021/11/05/eua-oferecem-10-milhes-dolares-informacoes-ransomware-darkside/ ; acesso em 28 jul 2022.

BRANCO, Dácio Castelo. **FBI alerta sobre ataque ransomware que afetou 30 empresas dos EUA em 2021**. 26 out 2021. Disponível em:

https://canaltech.com.br/seguranca/fbi-alerta-sobre-ataque-ransomware-que-afetou-30-empresas-dos-eua-em-2021-199963/ ; acesso em 06 jul 2022.

BRITO, Douglas Roberson de. Combatendo **a ameaça ransomware aplicando a norma NBR ISO/IEC 27001:2013 na gestão da segurança da informação.** Monografia [Especialização em gestão de Tecnologia da Informação e Comunicação] apresentada ao Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná. Curitiba, PR. 2016. Disponível em:

http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/19456/1/CT_GETIC_V_2015_07.pdf; acesso em 06 jul 2022.

CARVALHO, Henrique Carlos Fonte Boa; PELLI, Eduardo. **Técnicas de reconhecimento de padrões para identificação de ataque de DNS**. Revista Brasileira de Computação Aplicada (ISSN 2176-6649), Passo Fundo, vol. 9, n. 2, p. 99-110, jul. 2017. Disponível em: http://seer.upf.br/index.php/rbca/article/view/6279/4288; acesso em 13 jul 2022.

FIREEYE. **Visualização de ataques ransomware em tempo real**. 2022. Disponível em: https://www.fireeye.com/cyber-map/threat-map.html; acesso em 06 jul 2022.

*FORNASIER, Mateus de Oliveira; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina.* **Ransomware e cibersegurança: a informação ameaçada por ataques a dados**. Recista Thesis Juris. E-ISSN: 2317.3580. 20 mai 2020. Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/16739; acesso em 11 jul 2022.

GAFETY. **O que é RaaS (Ransomware as a Service)?** Artigo publicado em 23 mar 2021. Disponível em: https://gatefy.com/pt-br/blog/o-que-e-raas-ransomware-as-a-service/; acesso em 28 jul 2022.

KASPERSKY LAB. **O que é o ransomware WannaCry**? 2022A. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry; acesso em 27 jul 2022.

KASPERSKY. **O que são ataques de DDoS**? 2022B. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ddos-attacks; acesso em 28 jul 2022.

KOK, Sim Hoong; ABDULLAH, Azween; JHANJHI, Noor Zarman; SUPRAMANIAM, Mahadevan. **Prevenção de Crypto-Ransomware usando um Algoritmo de Detecção de Criptografia.** Computadores, nov. **2019**, *8*, 79; doi:10.3390/computadores8040079. Disponível em: http://paper.ijcsns.org/07_book/201902/20190217.pdf; acesso em 27 jul 2022.

KUMARI, Anjali; BHUIYAN, Md Zakirul Alam; NAMDEO, Jigyasa; KANAUJIA, Shipra; AMIN, Ruhul; VOLLALA, Satyanarayana. Proteção contra ataques de resgate: Uma Abordagem Criptográfica. Springer Nature Switzerland AG 2019. G. Wang *et al*. (Eds.): SpaCCS 2019, LNCS 11611, pp. 15-25, 2019.

https://doi.org/10.1007/978-3-030-24907-6_2; acesso em 27 jul 2022.

LAVADO, Thiago. **JBS pagou US$ 11 milhões em resgate a autores de ataque ransomware.** Matéria publicada em 09 jun 2021. Disponível em: https://exame.com/tecnologia/jbs-pagou-us-11-milhoes-a-autores-de-ataque-de-ransomware/; acesso em 06 jul 2022.

LEMA, Markus Carpeggiani de; FREITAS, Marcio. **Ataques Ransomware.** 5º. Seminário de tecnologia, Gestão e Educação. III Jornada Acadêmica & Simpósio de Egressos. ISSN 2675-1623. Faculdade e Escola Técnica Alcides

Maya. Rio Grande do Sul – maio 2021. Disponível em:

http://raam.alcidesmaya.edu.br/index.php/SGTE/article/view/326/318; acesso em 11 jul 2022.

LYNGAAS, Sean. **Sistema de saúde da Flórida é invadido e dados de 1,3 milhão são expostos**. 04 jan 2022. Disponível em: https://www.cnnbrasil.com.br/tecnologia/sistema-de-saude-da-florida-e-invadido-e-dados-de-13-milhao-sao-expostos/; acesso em 28 jul 2022.

MARIETTO, Maria das Graças Bruno. **Sociedade da Informação e Geografia do Ciberespaço.** INTERAÇÕES Revista Internacional de Desenvolvimento Local. vol. 2, n. 3, p. 29-36, set. 2001.

MARTON, Fábio. **Anonymous descobre que "ataque ransomware" ao Ministério da Saúde era outra coisa; PF confirma.** 10 dez 2021. Disponível em:

https://olhardigital.com.br/2021/12/10/seguranca/anonymous-pf-ransomware-ministerio-saude/; acesso em 06 jul 2022.

MASSENO, Manuel David; WENDT, Emerson. **O ransomware na lei: apontamentos breves de direito português e brasileiro.** Revista Eletrônica Direito & TI, vol. 1, n. 8, 2017. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/80; acesso em 11 jul 2022.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco; BATISTA JR, Eliezer; ROCHA, Henrique Ribeiro da. **O uso do ciberespaço pela administração pública na pandemia da COVID-19: diagnósticos e vulnerabilidades**. Revista de Administração Pública. Rio de Janeiro, vol. 54, n. 4, p. 650-662, jul. - ago. 2020. Disponível em: https://www.scielo.br/j/rap/a/x3VKDBRYpkvNb8dmXN4rNyR/?lang=pt&format=pdf; acesso em 06 jul 2022.

MITRA, Amrita. **What is ARP Spoofing**? **Figura 5**. Publicada em março de 2017. Disponível em: https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-arp-spoofing/; acesso em 28 jul 2022.

OLIVEIRA, Jéssica Cristina de. **Ransomware - Laboratório de Ataque do WannaCry**. Monografia [graduação em Engenharia de Software] apresentada à Universidade de Brasília - UnB Faculdade UnB Gama - FGA Engenharia de Software. Nov. 2018. Disponível em: https://bdm.unb.br/bitstream/10483/23052/1/2018_JessicaCristinaDeOliveira_tcc.pdf; acesso em 11 jul 2022.

OWAIDA, Amer. **Agência de cibersegurança dos EUA adiciona a autenticação de fator único à lista de práticas inadequadas**. Matéria publicada em 20 Oct 2021. Disponível em: https://www.welivesecurity.com/br/2021/10/20/agencia-de-ciberseguranca-dos-eua-adiciona-a-autenticacao-de-fator-unico-a-lista-de-praticas-inadequadas/; acesso em 06 jul 2022.

PEREIRA, Nicholas de Lucas Bastos; NEVES, Lucas Miranda. **Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus).** Revista Tecnológica Fatec Americana, vol. 9, n. 01. 31 ago 2021. Disponível em: DOI: 10.47283/244670492021090167; Acesso em 11 jul 2022.

PHILOT, Daniel Rocha. **Segurança da Informação: Ataques Ransomware e Proteção de Dados**. Relatório de pesquisa na modalidade de Estudo de Caso apresentado ao Curso de Tecnólogo em Gestão da Tecnologia da Informação da Universidade do Sul de Santa Catarina. Palhoça (SC), 2021. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/17754/1/DANIEL_ROCHA_PHILOT-Estudo_Caso-2021.pdf; acesso em 11 jul 2022.

PIMENTEL, Jose Eduardo de Souza; CABRERA, Diego Antunes; FORTE, Cleberson Eugênio. **Ransomware: do surgimento aos ataques "as a service".** Congresso de Segurança da Informação das Fatec (FATEC SEG). I FatecSeg - Congresso de Segurança da Informação – 17 e 18 set 2021. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/44/4; acesso em 11 jul 2022.

PPLWARE. **Universidade com 157 anos fecha portas devido… a Ransomware.** Matéria publicada em 11 mai 2022. Disponível em: https://pplware.sapo.pt/informacao/universidade-com-157-anos-fecha-portas-devido-a-ransomware/; acesso em

PRIVACY TOOLS. **Tradicional universidade dos EUA, Lincoln College, fecha suas portas após um ataque ransomware. 2022. Disponível em:** https://www.privacytools.com.br/tradicional-universidade-dos-eua-lincoln-college-fecha-suas-portas-apos-um-ataque-ransomware/; acesso em 06 jul 2022.

SILVA, Daniel Neves. **Guerra Fria**. 2022. Disponível em: https://mundoeducacao.uol.com.br/historiageral/guerra-fria.htm#:~:text=A%20Guerra%20Fria%20teve%20os,)%2C%20entre%201947%20e%201991; acesso em 12 jul 2022.

SILVA, Eduardo Araújo da. **Ciberespaço e Cibercultura: Definições e Realidades Virtuais Inseridas na Práxis do Homem Moderno**. 15 abr 2014. Disponível em: https://www.pedagogia.com.br/artigos/ciberespaco_cibercultura/index.php?pagina=3; acesso em 13 jul 2022.

SONICWALL. **Visualização de ataques ransomware em tempo real**. 2022A. Disponível em: https://attackmap.sonicwall.com/live-attack-map/; acesso em 06 jul 2022.

TECMUNDO – **Ataque de ransomware desligou portas automáticas de prisão nos EUA**. 11 jan 2022. Disponível em: https://www.tecmundo.com.br/seguranca/231807-ataque-ransomware-desligou-portas-automaticas-prisao-eua.htm; acesso em 06 jul 2022.

TIC NEWS. **Senado norte-americano aprova pacote de cibersegurança**. 10 03 2022. Disponível em: https://www.apdc.pt/noticias/atualidade-internacional/senado-norte-americano-aprova-pacote-de-ciberseguranca; acesso em 29 jul 2022.

Enviado: Agosto, 2022.

Aprovado: Agosto, 2022.

[1] Tecnólogo em Gestão da Tecnologia da Informação. ORCID: 0000-0002-5179-3114.