A PROFECIA *RANSOMWARE* E O FENÔMENO CIBERNÉTICO DA EXTORSÃO CRIPTOVIRAL

RANSOMWARE PROPHECY AND THE CYBER PHENOMENON OF CRYPTOVIRAL EXTORTION

RENATO TEIXEIRA REZENDE
Promotor de Justiça

Resumo: O presente artigo tem por escopo expor e analisar o fenômeno cibernético e os efeitos socioeconômicos e criminais da extorsão criptoviral, manifestados pela evolução e sofisticação da ferramenta maliciosa denominada *ransomware*, empregada por agentes criminosos na execução de ataques eficientes. As pesquisas foram desenvolvidas com bases em livros, artigos científicos, teses e materiais audiovisuais disponíveis on-line, sobre a construção histórica e a prova de conceito do *ransomware*, sem descurar do atual cenário de explosão de crimes cibernéticos no Brasil, em plena pandemia de Covid-19, que exigiu, dos setores públicos e privados, novas arquiteturas de rede, interconectividade e meios eletrônicos para garantir continuidade dos serviços, das operações e dos negócios, aumentando as superfícies de vulnerabilidades *zero-day*. Pretende-se, também, alertar para a necessidade da criação e da capacitação de forças tarefas coordenadas para o combate aos criminosos cibernéticos, com destaque para a implantação e desenvolvimento de novas ferramentas investigativas.

Palavras-chave: *ransomware;* extorsão criptoviral; direito penal.

Abstract: This article aims to expose and analyze the cyber phenomenon and the socioeconomic and criminal effects of cryptoviral extortion, manifested by the evolution and sophistication of the malicious tool called ransomware, used by criminal actors in the execution of efficient cyber attacks. The researches were developed based on books, scientific articles, theses and audiovisual materials available online, on the historical construction and proof of concept of ransomware, without neglecting the current scenario of explosion of cybercrimes in Brazil, in the midst of Covid-19 pandemic, which required new network architectures, interconnectivity and electronic means from the public and private sectors to ensure continuity of services, operations and business, increasing the surfaces of zero-day vulnerabilities. It is also intended to alert to the need for the creation and training of coordinated task forces to combat cyber criminals, with emphasis on the implementation and development of new investigative tools.

Keywords: ransomware; cryptoviral extortion; criminal law.

1. Introdução

Em meados do ano de 1995, na fase primitiva da *internet*, quando o acesso ao público leigo era deveras reduzido e interessados dependiam, para interação digital, de barulhentos *modens dial-up* e conexões telefônicas para o uso de sistemas de *e-mail* e *chats* em rudimentares servidores BBS,[1] Adam L. Young e Moti Yung (2017) se reuniram em um dos laboratórios do Departamento de Ciência da Computação da Universidade de Columbia e cogitaram a seguinte questão: quão devastador poderia ser o mais furtivo, traiçoeiro e malicioso *software* contra um dispositivo informático? Em outros termos, como seria e atuaria o mais poderoso vírus de computador? Até aquela data, o mundo havia experimentado o primeiro ataque de *cryptotrojan* em 1989, com a disseminação da praga digital conhecida como *AIDS Info Disk* ou *PC Cyborg Trojan* (FISCUTEAN, 2021). Os usuários receberam disquetes flexíveis contendo um *software* de questionário para mensuração dos riscos de contaminação do vírus HIV, causador da AIDS. Todavia, o programa ocultava um *Cavalo de Troia* (*trojan horse*). Após certo número de reinicializações, o *malware* insidioso criptografava os arquivos do computador hospedeiro e lançava um aviso na tela para que as vítimas adquirissem a licença anual ou vitalícia por determinado valor em dólar, caso quisessem desbloquear (descriptografar) os dados. Pela primeira vez os usuários se depararam com um "sequestro de dados" e uma extorsão criptoviral em um mundo que engatinhava na tecnologia cibernética.

Contudo, os arquivos foram facilmente desbloqueados, tendo-se em conta que o autor do *malware* utilizou uma chave simétrica, que permitia ser descoberta pela engenharia reversa do código binário do *trojan* e a sua consequente descriptografia. Na sequência, forças policiais de diversas partes do mundo lograram êxito em rastrear e localizar o autor da praga maliciosa, prendendo-o. Deparando-se com esse caso, os pesquisadores Adam L. Young e Moti Yung não só perceberam a potencialidade nociva do desenvolvimento de pragas virtuais dessa natureza, como vaticinaram o perigo real do uso da criptografia como instrumento lesivo e de consequências devastadoras. Nesse contexto, a *Criptovirologia* nasceu da curiosidade científica sobre o que o futuro reservava para os

1"Um *Bulletin Board System* (BBS) era um sistema informático (*software*) que permitia a conexão discada, via telefone, a um sistema externo, por meio de dispositivo de computador e interagir com ele, tal como hoje se faz com a *internet*. [...] Além de proporcionar a distribuição de *softwares*, aplicativos, informações e lazer, como jogos *online*, os BBSs eram usados por empresas que precisavam integrar seus funcionários externos. Com um computador, às vezes um *laptop*, e um telefone, o usuário conseguia enviar os pedidos de vendas, relatórios e interagir com os dados da empresa, com custos relativamente baixos. Hoje em dia isso é simples com a *internet* e o hipertexto nos documentos". (BULLETIN, 2021)

ataques cibernéticos criminosos que mesclam programação de *malware* com tecnologia criptográfica de ponta (YOUNG; YUNG, 1996). Pode-se dizer que a *Criptovirologia* está para a penetração ou a violação de sistemas de computador como a *Criptoanálise* está para a quebra de códigos (YOUNG; YUNG, 2004, p. 22). Por meio de "prova de conceito", os pesquisadores criaram um *malware* em ambiente seguro de laboratório e provaram, na prática, a teoria da extorsão criptoviral: o infrator coloca uma chave criptográfica pública na programação do código do *malware*, enquanto mantém, em sigilo, a chave privada de descriptografia.

O *malware* gera uma chave simétrica aleatória, que é usada para criptografar os dados da vítima, armazenados no dispositivo informático. Ato contínuo, essa chave simétrica é criptografada com a chave pública. Após a infecção do hospedeiro e o "sequestro" dos arquivos, o vírus digital zera a chave simétrica e o texto simples e, em seguida, coloca uma nota de resgate contendo o texto cifrado assimétrico e um meio para entrar em contato com o invasor. Para cada dispositivo "sequestrado", gera-se uma chave aleatória, de modo que um eventual acesso à chave daquele que pagou o "resgate" não servirá para descriptografar ("libertar") os dados de outras vítimas. As chaves criptográficas não poderiam ser extraídas do isolamento do vírus digital e do emprego de engenharia reversa. Se o vírus se espalhasse para diversos hospedeiros, as consequências seriam catastróficas. Ainda no ano de 1996, com a apresentação da hipótese e das pesquisas no Simpósio IEEE sobre Segurança e Privacidade, a dupla de autores previu que esse tipo de ataque seria ainda mais devastador com o surgimento das "moedas eletrônicas", quatorze anos antes do surgimento do *bitcoin* e do *blockchain*.

A expressão "extorsão criptoviral" se converteu em *ransomware* por imposição da mídia, que cunhou esse termo quando os ataques se tornaram uma realidade brutal a partir de 2010. Os pesquisadores sofreram uma espécie de *Maldição de Cassandra*,[2] uma vez que profetizaram o perigo concreto da extorsão criptoviral, demonstrando o conceito para o mundo, mas ninguém acreditou nas previsões. Décadas após o vaticínio, o mundo é aterrorizado pelas ondas de ataques cibernéticos destrutivos, cada vez mais específicos e direcionados, com o emprego insidioso de *ransomwares*. No ano de 2020, o Brasil não só é o segundo país com o maior número de ataques cibernéticos, como também se tornou celeiro de desenvolvimento, uso, locação e disseminação dessas pragas digitais, empregadas por criminosos em invasões direcionadas, como ferramentas para a extor-

2 Cassandra, personagem da mitologia grega, filha do rei Príamo e da rainha Hécuba, de Troia, previu o desastre da Guerra de Troia para o povo troiano, mas foi desacreditada e tida por louca, em razão de um desentendimento com o deus Apolo. Troia foi então vencida pelos gregos.

são das vítimas e a obtenção de vantagens econômicas ilícitas. Nesse cenário de explosão da criminalidade digital, o Ministério Público e as forças de segurança não podem ignorar o perigo real e imediato.

2. O *software* malicioso

No universo da segurança da informação, *malware*[3] é uma terminologia utilizada para descrever um *software* malicioso, caracterizado pela furtividade, desenvolvido por agentes criminosos para interromper as operações ou atividades, provocar danos ou obter acesso a computadores, sistemas informatizados ou redes de equipamentos informáticos, sem o conhecimento ou permissão de usuário ou de administradores. Em outros termos, *malware* pode ser definido como qualquer *software* intencionalmente projetado para causar danos a um computador, servidor, cliente ou rede de computadores, terminologia que distingue tais programas dos *bugs de software*, ou seja, danos, alterações ou corrupções de programas ou sistemas operacionais legítimos, causados por defeitos, falhas ou erros de programação não desejados pelos fabricantes, desenvolvedores ou programadores. *Malware* tornou-se um termo genérico usado para descrever todos os tipos de *softwares* considerados hostis, mal-intencionados ou invasores de sistemas ou de redes de computadores.

Constituem exemplos de programas maliciosos, os vírus cibernéticos, *worms*, *droppers*, *trojans* (Cavalos de Troia), *rootkits*, *bootkits*, *keyloggers*, *ransomwares*, *spywares*, *adwares*, *scarewares* e outros programas mal-intencionados, linhas de código ou *scripts* análogos. Na atualidade, pode-se afirmar que inexistem equipamentos eletrônicos ou de informática, *softwares* ou aplicativos de dispositivos móveis ou de IoT (*Internet of Things*), ainda que produzidos pela mais alta tecnologia militar, invulneráveis ou imunes às ameaças de infecção e às atividades insidiosas ou destrutivas de *malwares*. Insta salientar que os *malwares* compartilham inegáveis semelhanças com as doenças biológicas causadas por micro-organismos patogênicos (vírus, bactérias, fungos, protozoários, etc.) (GROOT, 2020). Devido a essas semelhanças, os pontos de entrada considerados são comumente chamados de "vetores", assim como no mundo da epidemiologia, que usa esse termo para designar os agentes portadores/transmissores de patógenos prejudiciais à saúde. Como no mundo dos organismos biológicos, existe uma gama de métodos, meios e modos de corromper os sistemas e de curá-los (ou resgatá-los).

3 *Malware* é a abreviatura de *malicious software* e é normalmente usada como um termo para se referir a qualquer *software* projetado para causar danos a um único computador, servidor ou rede de computadores, seja um vírus, *spyware*, etc. Para outras definições, ver Moir (2009).

Em linhas gerais, vírus podem ser definidos como programas de computador ou *scripts*[4] que tentam se espalhar de um arquivo para outro em um único computador e/ou de um computador para outro, usando uma variedade de métodos, sem o conhecimento e consentimento do usuário (vítima). Um vírus é um código malicioso executável que está anexado a outro arquivo executável, como um programa legítimo. A maioria dos vírus necessitam da iniciativa do usuário (vítima) e podem ser programados para execução (operação) em hora ou data específica. Os vírus de computador geralmente são transmitidos por meio de mídias ou dispositivos removíveis (HD externo, *pendrives*, disquetes, cartões de memória, etc.), *downloads* de arquivos disponíveis na *internet*, anexos de e-mails ou em virtude de vulnerabilidades de aplicativos ou de sistemas operacionais.

Hodiernamente, os vírus são projetados e potencialmente perigosos para a quase totalidade dos dispositivos eletrônicos e de informática, incluindo os móveis (celulares, *notebooks*, *smartphones*, *tablets*, câmeras fotográficas, consoles portáteis, roteadores, dispositivos de IoT, etc.). Os vírus podem ser inofensivos e apenas exibir uma imagem na tela (memes ou pornografia) ou podem ser destrutivos, como aqueles que modificam, sequestram ou excluem sistemas, programas e arquivos. Para evitar a detecção, o vírus sofre mutações ou é auxiliado pela camuflagem de *rootkits*.[5] O simples ato de abrir um arquivo pode ativar um vírus, infectando sistemas operacionais, setores de *boot*, *pendrives* conectados em portas USB, discos rígidos, roteadores, *switches*, modens, *smartphones*, etc. A execução de um programa específico, como, por exemplo, um jogo *online* ou editor de textos, pode ativar um vírus instalado no sistema. Uma

---

4 Segundo o verbete da *Wikipedia* sobre "linguagem de *script*": "Linguagem de *script* ou *scripting* é uma linguagem de programação que suporta *scripts*, programas escritos para um sistema de tempo de execução especial que automatiza a execução de tarefas que seriam executadas, uma de cada vez, por um operador humano. Linguagens de *script* são frequentemente interpretadas (ao invés de compiladas). Primitivas são frequentemente as tarefas elementares ou chamadas de API, e a linguagem permite a elas serem combinadas dentro de programas complexos. Os ambientes que podem ser automatizados através de *scripting* incluem aplicações de *software*, páginas *web* dentro de um navegador *web*, os *shells* de sistemas operacionais (OS), sistemas embarcados, bem como numerosos games. Uma linguagem de *script* pode ser vista como uma linguagem de domínio específico para um ambiente particular (no caso do *scripting*, uma aplicação também conhecida como uma "linguagem de extensão")".

5 "Um *rootkit* é um programa de computador clandestino projetado para fornecer acesso privilegiado contínuo a um computador enquanto oculta ativamente sua presença. O termo *rootkit* é uma junção das duas palavras *root* e *kit*. Originalmente, um *rootkit* era uma coleção de ferramentas que permitia o acesso de nível de administrador a um computador ou rede. *Root* se refere à conta *Admin* em sistemas Unix e Linux, e *kit* se refere aos componentes de *software* que implementam a ferramenta. Hoje, os *rootkits* são geralmente associados a *malware* - como Cavalos de Troia, worms, vírus - que ocultam sua existência e ações dos usuários e outros processos do sistema. [...] Um *rootkit* permite que alguém mantenha o comando e controle sobre um computador sem que o usuário/proprietário do computador saiba disso. Depois que um *rootkit* é instalado, o controlador do rootkit tem a capacidade de executar arquivos remotamente e alterar as configurações do sistema na máquina *host*. Um *rootkit* em um computador infectado também pode acessar arquivos de *log* e espionar o uso legítimo do proprietário do computador." (ROOTKIT, 2021, tradução minha)

vez ativo, o vírus normalmente afetará outros programas no computador ou outros dispositivos conectados à infraestrutura de rede. Com efeito, o presente artigo tem por escopo circunscrever a pesquisa e a discussão sobre os *ransomware* que, embora possam ser considerados, por definição, como vírus cibernéticos, possuem características, funcionalidades e finalidades específicas.

3. A criptovirologia e a evolução do *ransomware*

3.1. O *modus operandi* da ferramenta de ataque

Ransom (sequestro) *software* (programa de computador), conhecido pela abreviatura *ransomware*,[6] é um tipo de *malware* utilizado por criminosos cibernéticos como método insidioso para infectar os sistemas operacionais ou redes de computadores de usuários finais (indivíduos ou empresas) e criptografar arquivos, dados e sistemas, com o propósito de extorquir as vítimas, mediante emprego de grave ameaça e, assim, obter vantagem econômica ilícita. Não raro, os infratores que controlam remotamente ou utilizam o *ransomware*, após a infecção, instalação e a atividade de sequestro criptográfico de dados das vítimas, ameaçam torná-los públicos na rede mundial de computadores (ou em outros meios de comunicação) ou bloquear o acesso ao material capturado por tempo indeterminado, a menos que um resgate, com valor pré-determinado pelos agentes criminosos, seja pago a tempo e a modo.

Conquanto alguns *ransomwares* singelos possam bloquear os sistemas com métodos simples ou óbvios, não sendo difícil o emprego de engenharia reversa por indivíduos experientes, permitindo a rápida restauração ao *status quo ante*, variantes avançadas desse *malware* empregam técnicas criptográficas de chaves assimétricas, complexas e sofisticadas, conhecidas como *extorsão criptoviral*. A criptografia assimétrica,[7] utilizan-

6 Uma definição didática pode ser obtida em Ransomware (2021).

7 Segundo o verbete da *Wikipedia* sobre criptografia de chave pública: "Criptografia de chave pública, também conhecida como criptografia assimétrica, é qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que podem ser amplamente disseminadas, e chaves privadas que são conhecidas apenas pelo proprietário. Isto realiza duas funções: autenticação, onde a chave pública verifica que um portador da chave privada parelhada enviou a mensagem, e encriptação, onde apenas o portador da chave privada parelhada pode decriptar a mensagem encriptada com a chave pública. [...] Em um sistema de criptografia de chave pública, qualquer pessoa pode criptografar uma mensagem usando a chave pública do destinatário. Essa mensagem criptografada só pode ser descriptografada com a chave privada do destinatário. Para ser prática, a geração de uma chave pública e privada deve ser computacionalmente econômica. A força de um sistema de criptografia de chave pública depende do esforço computacional (fator de trabalho em criptografia) necessário para encontrar a chave privada de sua chave pública emparelhada. Segurança efetiva requer apenas manter a chave privada. A chave pública pode ser distribuída abertamente sem comprometer a segurança".

do chaves públicas e privadas, torna os arquivos, dados e sistemas inacessíveis ao usuário, compelindo-o ao pagamento do resgate exigido, para descriptografá-los e restaurá-los. Esse processo criptográfico equivale ao aprisionamento indefinido dos dados e à inutilização de sistemas. A depender do método de criptografia, com uso de algoritmos mais complexos, torna-se impossível para o usuário obter os meios necessários à descriptografia. Em alguns casos, esse processo demandaria bilhões de horas de esforços computacionais para descobrir as combinações da chave privada, resultando em inutilização perpétua de dados e sistemas, assim como enormes prejuízos financeiros e materiais para a recuperação do desastre. Como assinalado por Renan Cabral Saisse (2016), a peculiaridade de um *ransomware* em "se passar" por arquivos comuns impede a detecção por ferramentas antivírus tradicionais, elevando a sua periculosidade a um grau alarmante, considerando, ainda, o *modus operandi* agressivo quando executados, resultando no "sequestro de dados". O panorama dessas consequências nefastas, principalmente para o setor privado, gera indelével pressão psicológica nas vítimas, que, não raro, optam por pagar o resgate exigido pelos infratores, na esperança de recuperar o acesso aos arquivos e restaurar os sistemas indispensáveis à realização de operações críticas, máxime quando indivíduos e empresas não dispõem de sistemas seguros e eficientes de *backup* e de projetos de recuperação de desastres e de continuidade de negócios.

3.2. Da dificuldade de rastreamento dos infratores

Outro fator criminológico também é observado no padrão comportamental das vítimas: a intolerância econômica ao longo do tempo de paralisação das atividades e das operações. Isso ocorre em empreendimentos que operam 24 (vinte e quatro) horas e 07 (sete) dias da semana. Cada hora de suspensão das atividades representa perda considerável de receitas e aumento de despesas. Como definido pela *Cybersecurity and Infrastructure Security Agency* (CISA),[8] *ransomware* é uma forma de *malware* projetado para criptografar arquivos em um dispositivo, bloqueando ou inutilizando quaisquer arquivos e sistemas. Ato contínuo, os atores maliciosos exigem resgate em troca do fornecimento da chave privada (especifica e única) de descriptografia. Deve-se averbar que ine-

8 A CISA desenvolve a capacidade nacional de defesa dos Estados Unidos da América contra os ataques cibernéticos e trabalha com o governo federal para fornecer ferramentas de segurança cibernética, serviços de resposta a incidentes e recursos de avaliação para proteger as redes '.gov' que suportam as operações essenciais de departamentos e agências parceiros.

xiste garantia de que os criminosos cibernéticos forneçam as chaves privadas para descriptografia, ainda que tenham acesso ao valor pago pelo resgate, circunstância que incrementa o risco da decisão da vítima. Além da metodologia criptográfica utilizada pelos cibercriminosos no desenvolvimento do *ransomware*, o inegável sucesso da ferramenta maliciosa advém da forma como os resgates são extorquidos.

Na fase primitiva da *internet*, infratores exigiam o pagamento em dinheiro físico, transferências para contas bancárias em paraísos fiscais, carregamento de cartões de crédito pré-pagos, entre outras transações caracterizadas pela célere rastreabilidade pelos órgãos multilaterais e forças tarefas de investigação e vigilância financeira. Com o surgimento do *CryptoLocker*, em 2013, os infratores passaram a exigir das vítimas que adquirissem criptomoedas em carteiras eletrônicas, como, por exemplo, o *bitcoin* e o *moneros*. Esse método de obtenção de vantagem econômica ilícita trouxe o poder do anonimato aos criminosos e a extrema dificuldade de rastreamento do destino da criptomoeda. A conjunção desses elementos (criptografia e anonimato), assim como o intercâmbio de conhecimentos e experiências em fóruns de discussão e redes sociais privadas que pululam na *darkweb*, fomentou a explosão do fenômeno criminológico da fabricação e uso de *ransomware*. Nos últimos anos, incidentes de *ransomware* têm se tornado cada vez mais presentes em entidades governamentais federais, estaduais e municipais de diversas Nações e organizações, públicas ou privadas, principalmente em relação à infraestrutura crítica. Incidentes de *ransomware* podem afetar severamente os negócios e deixar as organizações (públicas ou privadas) sem os dados de que precisam para operar e entregar serviços de missão crítica (saúde, assistência social, educação, transporte, finanças, produção e logística de alimentos, abastecimento de água, energia elétrica, atividades militares, etc.). Com a eficácia de ataques dessa natureza, os valores das extorsões se tornaram elevados, atingindo a marca de milhões de dólares. As atividades com *ransomware* inauguraram uma nova fase das ameaças cibernéticas mundiais, o *malware as a servisse* (VILLADIEGO, 2020), ou seja, o desenvolvimento, a venda ou a locação de *softwares* maliciosos por determinados infratores, em geral em transações camufladas pela *deepweb* ou *darkweb*, para outros grupos criminosos, surgindo um mercado clandestino altamente lucrativo de *extorsão criptoviral*. Alguns invasores sofisticados estão desenvolvendo *kits* de ferramentas que podem ser baixados e implantados por invasores com menos habilidades técnicas, para execução de crimes cibernéticos.

3.3. Da pandemia de *ransomware*

Alguns dos cibercriminosos mais avançados estão monetizando o *ransomware* (GROOT, 2020), fenômeno representativo do aumento da proeminência de *ransomwares* conhecidos como *CryptoLocker* (KELION, 2013), *CryptoWall*,[9] *Locky* (PAUL, 2016), e *TeslaCrypt*.[10] Estes são alguns exemplos de tipos comuns de *malware* avançado. Estima-se que o *CryptoWall*, por exemplo, gerou mais de US$ 320.000.000,00 (trezentos e vinte milhões de dólares) em lucros ilícitos distribuídos entre os atores da cadeia criminosa, no período de atuação global. Todavia, um dos ataques mais perversos de *ransomware* advém do *Wannacry*,[11] que se iniciou em maio de 2017. O *malware* tinha como alvos computadores que executavam o sistema operacional *Microsoft Windows*, criptografando dados e exigindo pagamentos de resgate na criptomoeda *Bitcoin*. É considerado um *worm* de rede porque também inclui um mecanismo de transporte para se espalhar automaticamente, sem a necessidade de intervenção do usuário. Em outros termos, o código malicioso procurava por sistemas operacionais vulneráveis, geralmente desprovidos de atualizações, se instalava e iniciava a autorreplicação, espalhando-se lateralmente pelas redes para contaminar outros dispositivos, independentemente da atuação dos usuários finais.

Fontes constataram que o *Wannacry* atingiu as redes hospitalares do *National Health Service* (serviço público de saúde) na Inglaterra e na Escócia, sendo que aproximadamente setenta mil dispositivos, incluindo computadores, escâneres de ressonância magnética, geladeiras para armazenamento de sangue e equipamentos médicos podem ter sido afetados.[12] Em 12 de maio de 2017, alguns serviços do *National Health Service* tiveram que recusar emergências não críticas e algumas ambulâncias foram desviadas. Em 2018, um relatório de membros do Parlamento Britânico concluiu que todos os duzentos hospitais do sistema público de saúde, assim como outras organizações, meses após o ataque brutal do *Wannacry*, ainda eram falhos e deficientes em segurança cibernética

9 "É uma forma particularmente desagradável de *ransomware*. Ele faz muito mais que apenas criptografar os arquivos e solicitar que a vítima pague pela chave. Ele tenta se esconder dentro do sistema operacional e se adiciona a pasta Inicializar. Pra piorar, o *CryptoWall* exclui cópias de sombra de volume dos arquivos, tornando difícil restaurar os dados". (BERTOLLI, 2018) Veja o excelente artigo *Cryptowall* em 2018, para entender o avanço dessa ameaça cibernética.

10 Cf. TROJAN.TeslaCrypt.

11 Para o aprofundamento dos estudos, recomenda-se o documentário "A Arma Perfeita" (The Perfect Weapon). Direção de John Maggio. Estados Unidos: HBO Max, 2020. Duração: 87 min.

12 Cf. Global, 2017.

(SMYTH, 2018). Nissan Motor Manufacturing *UK* em Tyne and Wear, Inglaterra, interrompeu a produção depois que o *ransomware* infectou alguns de seus sistemas. A Renault também interrompeu a produção em vários locais na tentativa de impedir a disseminação do *ransomware* (SHARMAN, 2017). As empresas Telefónica, FedEx e Deutsche Bahn foram atingidas, junto com muitos outros países e empresas em todo o mundo (LARSON, 2017). De acordo com a empresa de modelagem de risco cibernético Cyence, as perdas econômicas com o ataque cibernético podem chegar a quatro bilhões de dólares, com outros grupos estimando que as perdas sejam da ordem de centenas de milhões (BERR, 2017).

No dia 9 de setembro de 2020 (O'NEILL, 2020), um ataque de *ransomware* em uma rede hospitalar, na Alemanha, resultou na provável morte de uma paciente em Düsseldorf, que estava programada para passar por cuidados intensivos. Em virtude do impacto do *ransomware* no hospital, a paciente foi transferida para outra unidade, distante trinta quilômetros. A paciente faleceu no deslocamento. Repetindo a proeza do *Wannacry*, surgiu a ameaça *Ryuk*, que afetou drasticamente as unidades médicas e hospitalares do *Universal Health System* nos Estados Unidos da América, em 27 de setembro de 2020, resultando no desvio de ambulâncias, interrupção de procedimentos, falhas e atrasos no acesso a dados e exames clínicos e laboratoriais, fazendo com que as urgências e emergências retornassem à utilização, ainda que provisória, de formulários, cadastros e registros em papéis e documentos físicos, para assegurar a continuidade dos serviços médicos. Na mesma esteira, foram os efeitos devastadores globais do *ramsonware NotPetya*, que adquiriu o título de arma cibernética, tendo em vista ter sido projetado por *hackers* patrocinados pela Rússia, para uso específico na Guerra da Ucrânia, no auge do conflito em 2017. De acordo com o Andy Greenberg (2018), horas após a primeira aparição em território ucraniano, o *worm* ultrapassou as fronteiras da Ucrânia e se espalhou em inúmeras máquinas ao redor do mundo, de hospitais na Pensilvânia (Estados Unidos da América) a uma fábrica de chocolate na Tasmânia (Oceania). O *malware* paralisou empresas multinacionais, incluindo a gigante logística Maersk, a farmacêutica Merck, a subsidiária europeia da FedEx, TNT Express, a construtora francesa Saint-Gobain, a produtora de alimentos Mondelēz e a fabricante Reckitt Benckiser (GREENBERG, 2019). Em cada caso, infligiu custos de nove dígitos. Até se espalhou para a Rússia, atingindo a companhia petrolífera estatal Rosneft. Com a disseminação global da infecção cibernética, os danos materiais atingiram a cifra estratosférica de dez bilhões de dólares.

3.4. Das tendências da ameaça cibernética global

No cenário cibernético hodierno, há duas tendências que se destacam em se tratando de *ramsonware*: a) os ataques direcionados e orquestrados por grupos *Advanced Persistent Threat* (APT), contra alvos específicos;[13] b) o uso do *malware* como arma cibernética em conflitos regionais entre países, como instrumento eficaz em guerras híbridas (RADIN, 2017, p. 5-6). O recente Relatório de Ameaças Cibernéticas Netwrix 2020 revelou que uma em cada 03 (três) organizações de saúde sofreu ataque de *ransomware* durante os últimos meses, o que é o maior resultado entre todos os setores. A razão para taxas tão altas é fácil de compreender. O setor de saúde revelou-se como alvo preferencial para *hackers* que se dedicam aos ataques direcionados e persistentes, principalmente desenvolvedores e operadores de *ransomware*, dada a escassez de recursos na área de segurança cibernética e de maturidade das infraestruturas de tecnologia de informação, uso de sistemas operacionais obsoletos, ausência de efetiva capacitação dos recursos humanos (ponta a ponta) e a enorme pressão sobre exercida pela comunidade nacional e internacional no desenvolvimento de estratégias eficientes no enfrentamento do Covid-19. No momento, sistemas de saúde e hospitais concentram recursos materiais, financeiros e humanos para o atendimento de pacientes graves e que necessitam de internações e cuidados intensivos, não restando tempo suficiente e dinheiro para a evolução das defesas cibernéticas.

Aliás, a pandemia de Covid-19 também contribuiu para o incremento do perigo concreto de propagação de *ransomware* (JOYCE, 2020). O risco para os hospitais e os pacientes será agravado por outro aumento nas infecções, que sobrecarregará as unidades de atendimento, emergência e internações, deixando pouco espaço para erros estratégicos. Laboratórios de pesquisa que trabalham para desenvolver vacinas e tratamentos também foram alvos desses ataques específicos e direcionados, que tinham por finalidade a subtração de informações críticas sobre a evolução e a eficiência das pesquisas médicas e biológicas, provavelmente com o escopo de vendê-las, posteriormente, no mercado clandestino para organizações criminosas ou

13 "Uma ameaça persistente avançada (APT) consiste em um ataque cibernético prolongado e direcionado no qual um invasor (os grupos de invasores), patrocinados por Estados-Nação ou pelo crime organizado, obtém acesso a uma rede determinada e permanece sem ser detectado por um longo período de tempo, utilizando múltiplas e sofisticadas técnicas, táticas e procedimentos. Os ataques APT são empregados para espionagem e subtração de dados críticos ou sensíveis, em vez de causar danos à rede e aos computadores da organização alvo. Os ataques APT são normalmente direcionados a organizações em setores como defesa nacional, manufatura e indústria financeira, já que essas empresas lidam com informações de alto valor, incluindo propriedade intelectual, planos militares e outros dados de governos e organizações empresariais. O objetivo da maioria dos ataques APT é alcançar e manter o acesso contínuo à rede visada, em vez de entrar e sair o mais rápido possível. Como geralmente são necessários muitos esforços e recursos para realizar ataques de estilo APT, os hackers costumam selecionar alvos de alto valor, como Estados-Nações e grandes corporações, com o objetivo final de subtrair informações críticas e valiosas por um longo tempo." (tradução nossa). (ROSENCRANCE, 2020).

Estados-Nação, violando os direitos sobre propriedade industrial e intelectual. Mesmo quando a disponibilidade desses sistemas é crucial para aliviar o sofrimento humano em todo o mundo, os invasores cibernéticos não mostraram escrúpulos ou compaixão na execução dos ataques.

Noutro vértice, tem-se a falsa percepção de que as vítimas (indivíduos, empresas ou organizações), em geral, não realizam pagamentos das extorsões aos cibercriminosos, nas situações de ataque bem-sucedido com *ransomware*. Entretanto, pesquisas mais recentes revelaram números assustadores em relação àqueles que cederam às chantagens, adquiriram e transferiram criptomoedas às carteiras dos infratores, objetivando restaurar arquivos e sistemas bloqueados por criptografia assimétrica ou evitar vazamentos de dados críticos ou sensíveis na *internet* (VIJAVAN, 2020). A IBM, por exemplo, relatou que, em setembro de 2020, um em cada quatro ataques corrigidos pela equipe de resposta a incidentes, conhecida como *X-Force*, era relacionado a *ransomware*. Alguns ataques envolveram pedidos de resgate de mais de quarenta milhões de dólares.

Escolas e universidades se tornaram alvos de *ransomware*, em virtude da mudança para o ensino a distância e a adoção de ambientes de trabalho híbridos, como resultado da pandemia de Covid-19, aumentando a superfície de vulnerabilidades e a exposição aos ataques cibernéticos (SINGLETON, 2020). Há notícias de que instituições acadêmicas dos Estados Unidos (WOOD, 2020), que sofreram ataques de *ransomware* em agosto e setembro de 2020, pagaram resgates que variam de quatrocentos mil dólares a mais de um milhão de dólares, na esperança de que informações confidenciais sobre professores, alunos e pesquisas não fossem divulgadas ao público (MCKENZIE, 2020). Um em cada três ataques de *ransomware* que a IBM corrigiu em 2020 envolveu *Sodinokibi*, uma família de *ransomware* que substituiu o *GandCrab* de 2019 como a cepa de *ransomware* mais prolífica. A análise da IBM mostrou que os operadores do *Sodinokibi* consideraram as receitas da organização ou corporação (vítima) ao determinar o valor da extorsão, com resgates médios variando de 0,08% a 9,1% da receita anual da empresa alvo.

A somar-se a isso, as estatísticas revelaram que 36% das vítimas de *Sodinokibi* pagaram resgate em troca da descriptografia dos dados aprisionados pela ação do *malware*. Os ataques observados no ano de 2020 sugerem que os agentes de ameaças de *ransomware* estão procurando vítimas com baixa tolerância ao tempo de inatividade, como, por exemplo, os setores industriais. As organizações que exigem muito tempo de atividade podem perder milhões de dólares todos os dias devido à paralisação das operações administrativas e finalísticas. Portanto, é mais provável que essas vítimas paguem o resgate para recuperar o acesso aos dados e retomar as operações.

Ressalta-se que uma pesquisa encomendada pela Sophos,[14] com cinco mil gerentes de Tecnologia de Informação, divulgada em maio de 2020, revelou que 26% das vítimas de *ransomware* pagaram seus atacantes no ano passado. Mais da metade das organizações representadas na pesquisa relataram um ataque de *ransomware* nos últimos doze meses. Deve-se acrescentar que a Sophos descobriu que os incidentes de *ransomware* se tornaram qualitativamente mais graves no ano de 2020. Muitos dos relatos eram ataques baseados em servidor que exigiam mais esforço para implantar e buscavam criptografar ativos críticos de negócios de alto valor (VIJAVAN, 2020).

De acordo com a pesquisa supracitada, o Brasil está em segundo lugar no ranking de países mais atingidos por *ransomware* em 2020. Estimou-se que 65% das organizações foram alvo de ataques dessa natureza. Com a pandemia de Covid-19, diversas empresas, entidades, instituições e organizações, públicas ou privadas, que já não possuíam uma infraestrutura cibernética em estágio de maturidade, migraram, às pressas, para o que se convencionou *home office*, aumentando, sobremaneira, a superfície de ataque e as vulnerabilidades. Os recursos financeiros e materiais, ainda que abundantes em determinados setores (públicos ou privados), não são adequadamente alocados. As capacitações periódicas dos empregados, servidores, gestores e administradores são raras ou meramente formais. No setor público, por exemplo, não há investimentos em educação em segurança cibernética, de forma contínua e periódica. Outro fator relevante: o Brasil não dispõe de órgãos suficientes de investigação de crimes digitais e recursos de perícia digital forense. As cadeias de vestígios deixados pelos cibercriminosos são ignoradas, sem olvidar que as vítimas, em geral, não acionam os órgãos de segurança pública, mantendo os incidentes em absoluto sigilo e longe da imprensa. Salvo exceções no setor privado, os órgãos públicos não fazem investimentos na implantação da doutrina de *Threat Intelligence* (inteligência de ameaças) e coordenação interinstitucional de tratamento e resposta a incidentes, como ocorre em países desenvolvidos que adotaram a doutrina de *Cyber Kill Chain*.[15]

---

14 Cf. The State of Ransomware 2020: Results of an independent study of 5,000 IT managers across 26 countries. Sophos, 2020.

15 "*Cyber Kill Chain* (cadeia de eliminação cibernética) é um modelo guiado por inteligência, que se baseia em uma série de etapas que traçam os estágios (ou camadas) de um ataque cibernético, desde os estágios iniciais de reconhecimento até a exfiltração de dados. A cadeia de eliminação ajuda a compreender e combater infecções por *ransomware*, violações de segurança e ataques persistentes avançados (APTs). A Lockheed Martin derivou a estrutura da cadeia de destruição de um modelo militar - originalmente estabelecido para identificar, se preparar para atacar, engajar e destruir o alvo. Desde o seu início, a cadeia de destruição evoluiu, como modelo, para melhor antecipar e reconhecer ameaças internas, engenharia social, ransomware avançado e ataques inovadores." (HOSPELHORN, 2020, tradução nossa).

No mês de maio de 2017, dez tribunais brasileiros sofreram ataques cibernéticos de *ransomware*, com variantes do *Wannacry* (Tribunais de Justiça dos Estados de São Paulo, Alagoas, Espírito Santo, Maranhão, Minas Gerais, Pará, Rio Grande do Norte, Roraima e do Distrito Federal e o Tribunal Regional do Trabalho da 2ª Região) (LUCHETE; GALLI, 2017). Decorridos três anos após aquelas invasões, no dia 3 de novembro de 2020, os técnicos de segurança e tecnologia da informação do Superior Tribunal de Justiça foram surpreendidos com um ataque de *ransomware*, que atingiu, pelo menos, mil e duzentos servidores, criptografando dados (o acervo de processos e *e-mails*) e *backups*. No dia 5 de novembro de 2020, o Superior Tribunal de Justiça, reconhecido como instituição pioneira na digitalização processual, era virtualmente inexistente, com a paralisação geral das atividades jurisdicionais (ESCOSTEGUY, 2020c). O invasor deixou uma curiosa mensagem para que os responsáveis pelo tribunal entrassem em contato por e-mail anônimo, se quisessem a restauração dos dados sequestrados pelo *malware*, sem contudo estabelecer o valor do resgate (ESCOSTEGUY, 2020b). De acordo com a imprensa, um servidor responsável pelo monitoramento do *firewall* e da proteção dos sistemas do Superior Tribunal de Justiça tinha autorização para trabalhar em casa, provavelmente em razão da pandemia de Covid-19. A conexão remota (*home office*) com sistemas críticos constituiu a provável brecha para a invasão dos sistemas da corte (ESCOSTEGUY, 2020d). É provável que os ataques contra o Superior Tribunal de Justiça resultaram em perdas de dados, sendo que as atividades permaneceram suspensas até o dia 15/11/2020. Noticiou-se, ainda, que, no mesmo período, o Conselho Nacional de Justiça, o DataSUS (órgão do Ministério da Saúde) e o Governo do Distrito Federal sofreram tentativas de ataques com método idêntico ao usado na invasão do Superior Tribunal de Justiça (ESCOSTEGUY, 2020a). Essa sequência de ataques, sem olvidar aqueles que ocorreram contra o Tribunal Superior Eleitoral[16] durante as eleições municipais, expuseram a fragilidade dos órgãos e das instituições públicas aos ataques cibernéticos, principalmente aqueles empregados por *Advanced Persistent Threats* (APT).

Com a evolução dos ataques com *ransomware*, os cibercriminosos aprimoraram e diversificaram as táticas, técnicas e procedimentos de invasão e contaminação dos alvos. Os infratores deixaram de lado a antiga doutrina de "*spray and pray*",[17] para se dedicarem, cada vez mais, aos ataques específicos e direcionados, com prévia seleção das vítimas e

16 Cf. AMORIM (2020)

17 A expressão de língua inglesa pode ser traduzida, literalmente, como "espalhar e rezar", fazendo alusão às ações no atacado, caracterizadas como aleatórias, indiscriminadas e abrangentes, visando capturar o maior número de vítimas, independentemente de quem são os alvos (pessoas físicas ou jurídicas, órgãos públicos ou empresas privadas, nações, setores econômicos ou profissionais, civis ou militares etc.). Nos ataques cibernéticos primitivos com emprego de *ransomware*, os atores não se importavam com as vítimas e sequer dedicam tempo e recursos para coleta de informações precisas sobre elas.

reconhecimento da infraestrutura e das capacidades de defesa e reação dos alvos. No final de 2019, constatou-se que os *hackers* que fazem uso de ferramenta *ransomware* adotaram, como primeiro passo, o reconhecimento e a cuidadosa penetração dos sistemas vitimados, com prévia *exfiltração* de dados e informações relevantes e, sendo possível, infectam os sistemas de *backup*. Na sequência, os atacantes executam o *ransomware*, criptografando os dados armazenados nos sistemas, sequestrando-os. Ainda que as vítimas conseguissem recuperar os sistemas, eliminando a ameaça cibernética e com o subsequente recurso aos sistemas de *backups*, estariam expostas à chantagem de vazamento dos dados, previamente capturados pelos invasores no ataque persistente, na rede mundial de computadores.

Esse fator se tornou determinante para que várias vítimas cedessem à extorsão, haja vista os riscos concretos de danos irremediáveis à reputação de usuários, organizações e instituições atingidas. Como pode-se inferir, o pagamento do resgate não é garantia de que os dados sensíveis ou críticos subtraídos não sejam expostos ao público, ou de que os infratores não darão continuidade à extorsão, talvez em outra oportunidade, aproveitando-se da vulnerabilidade social, econômica e psicológica das vítimas, em uma sucessão indefinida de chantagens. Nos últimos doze meses, os agentes maliciosos por trás desses ataques também ficaram melhores na infiltração de redes corporativas, incluindo ataques de força bruta em interfaces de acesso remoto, como RDP (protocolo de acesso remoto) e *Virtual Private Nertworks* (VPN), ambientes de virtualizações, serviços e soluções em nuvem (*cloud computing*), uso de *malware* e *exploits* para obter uma posição inicial, emprego de *spear phishing*[18] e outras técnicas de engenharia social, e *botnets* para ajudar a espalhar o *ransomware* (STAFF, 2020). Nos ataques contemporâneos, é possível que uma parcela dos invasores cibernéticos e criminosos estejam utilizando o *ransomware* como manobra diversionista e, como *dinamite lógica*, ativam a praga cibernética na fase final do ataque, para ocultação dos vestígios da espionagem e da exfiltração de dados críticos, objetivos reais da invasão, criando sobrecarga e desorientação nas equipes de defesa e de resposta ao incidente, além de dificultar as futuras investigações pela perícia digital forense.

Como exposto por Sandra Joyce (2020) em recente artigo publicado no sítio da *FireEye*, em vez de visar a vítimas indiscriminadamente, os ope-

18 Técnicas de engenharia social direcionadas a instituições ou indivíduos específicos são denominadas de *spear phishing*. Consiste na coleção de detalhes e informação pessoais de modo a aumentar a probabilidade de sucesso dos atacantes, em ludibriar as vítimas. É considerada a técnica de *phishing* mais eficaz na atualidade, sendo responsável por 91% de ataques deste gênero. (Spear Phishers: Angling To Steal Your Financial Info, 2009).

radores estão explorando entidades, organizações ou empresas críticas com os meios e a motivação para pagar enormes resgates, em ataques direcionados e persistentes, orientados pela inteligência e divididos em fases. Uma vez que as redes são violadas, os operadores se movem lateralmente, com habilidade, através das redes das vítimas, excluindo ou criptografando *backups* se puderem encontrá-los nessa jornada. Em seguida, os infratores implantam o *malware* em sistemas confidenciais. O resultado é a eficiência da implantação e difusão de *ransomware*, guiada pela inteligência humana, em vez do método indiscriminado que afeta máquinas aleatórias. Obter acesso a sistemas críticos permite que os operadores de *ransomware* exijam valores de resgate mais altos e aumenta o senso de urgência para pagar. E, à medida que o criminoso procura uma presa mais crítica, as consequências se tornam mais terríveis, não apenas em termos econômicos. Atualmente, o *ransomware* se tornou uma indústria criminosa que gira bilhões de dólares.

Os *hackers* costumam ter como alvo empresas, bloqueando tecnologias e roubando dados antes de demandar até milhões de dólares em extorsão. Com o desenvolvimento da doutrina dos ataques persistentes, os invasores almejam permanecer no ambiente interno da rede, sem serem detectados e, assim, podem passar semanas ou meses explorando a infraestrutura em profundidade, tentando escalar privilégios, realizar movimentos laterais, implantar bombas lógicas e aproveitar as permissões subtraídas para enviar o *ransomware* para o maior número possível de dispositivos *endpoint*, aguardando o momento adequado para execução. Os criminosos cibernéticos também podem usar esse tempo para identificar recursos de rede críticos, como *backups* de sistema, segmentos de rede que armazenam dados confidenciais e outros sistemas importantes que podem ser usados para disseminar a ferramenta *ransomware*. O tempo também se tornou relevante para a eliminação dos vestígios do ataque que poderiam possibilitar futuros rastreamentos por expertos em perícia digital forense, assegurando a impunidade dos agentes infratores. Portanto, a pressa na execução do *payload* se tornou inimiga da perfeição do plano criminoso.

3.5. Da tipificação penal dos crimes cibernéticos e técnicas de investigação

Do ponto de vista repressivo, na remota hipótese de identificação dos autores de ataques cibernéticos com *ransomware*, eles poderão responder por extorsão (artigo 158, *caput*, do Código Penal – pena de reclusão

de quatro a dez anos) e invasão de dispositivo informático (artigo 154-A, *caput*, do Código Penal – pena de detenção de três meses a um ano e multa). Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta de invasão de dispositivo informático (artigo 154-A, § 1º, do Código Penal). Aumenta-se a pena em um sexto a um terço se da invasão resulta em prejuízo econômico (artigo 154-A, § 2º, do Código Penal). Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, a pena é reclusão de seis meses a dois anos, e multa, se a conduta não constitui crime mais grave (artigo 154-A, § 3º, do Código Penal). A pena será aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos (artigo 154-A, § 4º, do Código Penal).

A pena também poderá ser aumentada de um terço à metade, se o crime for praticado contra: a) Presidente da República, governadores e prefeitos; b) Presidente do Supremo Tribunal Federal; c) Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; d) dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (artigo 154-A, § 5º, do Código Penal). Caso haja concurso de agentes com vínculos duradouros e divisão social de tarefas na execução do ataque de *ransomware*, abra-se espaço para a incidência do crime de organização criminosa (artigo 1º, § 1º, da Lei n.º 12.850/2013 – considera-se organização criminosa a associação de quatro ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a quatro anos, ou que sejam de caráter transnacional – pena de reclusão de três a oito anos de reclusão e multa).

Todavia, nos crimes definidos no artigo 154-A do Código Penal, somente se procede mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (artigo 154-B do Código Penal). *In casu*, constata-se que o legislador infraconstitucional, de forma tímida, criminalizou as condutas de invasão de dispositivos informáticos, que podem gerar consequências gravíssimas às vítimas e à sociedade, em um mundo globalizado e amplamente conectado em uma realidade ci-

bernética, como se fossem infrações penais de menor potencial ofensivo. No caso da invasão de dispositivos ou sistemas de informática, abre-se a discussão se há hipótese de concurso material de crimes entre a extorsão e o ataque cibernético (artigo 69 do Código Penal) ou se ocorrerá a incidência do princípio da consunção, como nos casos envolvendo estelionato e falsificação de documentos.

Como lecionado por Cezar Roberto Bitencourt (2003, p. 135), pelo princípio da consunção, ou absorção, a norma definidora de um crime constitui meio necessário ou fase normal de preparação ou execução de outro crime. Há consunção quando o fato previsto em determinada norma é compreendido em outra, mais abrangente, aplicando-se somente esta. Na relação consuntiva, os fatos não se apresentam em relação de gênero e espécie, mas de *minus* e *plus*, de continente e conteúdo, de todo e parte, de inteiro e fração. A norma consuntiva constitui fase mais avançada na realização da ofensa ao um bem jurídico, aplicando-se o princípio *major absorbet minorem*. Assim, como a invasão e a execução do *ransomware* em sistemas informáticos é meio para se atingir a extorsão (crime-fim), mostra-se defensável a aplicação do princípio da consunção. Porém, os crimes de extorsão e de invasão de sistemas informáticos protegem bens jurídicos diversos. O primeiro se destina à proteção do patrimônio, ao passo que o segundo se destina à proteção da liberdade individual, da imagem, da intimidade e da vida privada das vítimas. Não bastasse a tutela de bens jurídicos diversos, deve-se ter em conta que o *ransomware* desenvolvido para a invasão não se exaure em uma única conduta, podendo ser utilizado, com eficiência, em outros crimes e contra vítimas diversas, com ou sem modificações do código de programação original. Nesse contexto, é igualmente defensável a pretensão de se aplicar a regra do concurso material de crimes, resultando, na hipótese de condenação dos agentes, na soma das penas dos tipos penais, incrementando a reprimenda final, salvo em relação ao artigo 154-A, § 3º, do Código Penal, que prevê, expressamente, que a norma incriminadora não será aplicada, quando da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido se a conduta não constitui crime mais grave.

Noutro vértice, caso os criminosos cibernéticos, no uso de *ransomware*, tenham por escopo causar lesão ou perigo de lesão à integridade territorial, à soberania nacional, ao regime representativo e democrático, à Federação, ao Estado de Direito e às pessoas dos Chefes dos Poderes da União, poderão responder por crimes previstos na Lei n.º 7.170/83

(Lei de Segurança Nacional), como, por exemplo, nas condutas de: a) comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos (artigo 13 e seguintes da Lei n.º 7.170/83); b) praticar sabotagem contra instalações militares, meios de comunicações, meios e vias de transporte, estaleiros, portos, aeroportos, fábricas, usinas, barragem, depósitos e outras instalações congêneres (artigo 15 e seguintes da Lei n.º 7.170/83); c) devastar, saquear, extorquir, roubar, sequestrar, manter em cárcere privado, incendiar, depredar, provocar explosão, praticar atentado pessoal ou atos de terrorismo, por inconformismo político ou para obtenção de fundos destinados à manutenção de organizações políticas clandestinas ou subversivas (artigo 20 da Lei n.º 7.170/83).

Em se tratando de métodos e meios de investigação, o Professor Doutor, Leonardo Perin Vichi (2021), em recente artigo, admoestou que, conquanto os dados como códigos-fontes, endereços IP (*Internet Protocol*) e carteiras de criptomoedas não permitem muitos avanços na elucidação da autoria de ataques cibernéticos com emprego de *ransomware*, o texto do "pedido de resgate", não raro, traz informações relevantes que permitem uma análise linguística e de perfilamento dos atores maliciosos. Com efeito, a construção de perfis linguísticos é realizada com o emprego de métodos da Linguística Aplicada, por meio dos quais conjuntos de marcadores individuais e únicos de uma pessoa podem ser detectados, seja para extrair informações sobre a idade, a origem, a escolaridade, a classe social, o gênero, etc., do atacante, seja para comparação de evidências para esclarecimento de autorias contestadas. No entanto, quando faltam as evidências linguísticas diretas presentes em ataques de extorsão criptoviral, em se tratando especificamente de amostras como pedidos de resgates, manifestos e outros textos, é possível, ainda, proceder com outro tipo de análise linguística: a da estruturação lógica utilizada no código-fonte. Cada programador possui uma espécie de impressão digital ou idiossincrasia, definida pela forma como o agente organiza o próprio algoritmo e, por isso, os códigos-fontes são também importantes evidências que permitem levantar a idade, a origem e outras informações dos indivíduos que se ocultam por trás dos códigos maliciosos. Nesse compasso, é indubitável que a Linguística Forense poderá ser aprimorada como relevante instrumento de inteligência cibernética e de investigação no Direito Processual Penal.

4. Considerações finais

Abstrai-se que o fenômeno *ransomware* deixou de ser apenas um incômodo isolado, inofensivo ou representativo das literaturas de ficção científica ou de fantasia distópica. Trata-se de ameaça global em ascensão, com reflexos diretos no Brasil, onde grupos de criminosos cibernéticos estão adquirindo conhecimentos e intercambiando experiências para incrementar a eficiência de ataques direcionados e destrutivos, caracterizados, cada vez mais, pelo uso de etapas de inteligência e persistência. A pandemia de *ransomware* também revelou a fragilidade das infraestruturas críticas à ação de códigos maliciosos, com efeitos devastadores para os setores públicos e privados. Com a pandemia de Covid-19, os ataques com emprego de *ransomware* se tornaram frequentes e mais agressivos, com especial destaque para os órgãos que integram o sistema judiciário brasileiro. De averbar que ataques avançados dessa natureza trarão consequências trágicas, como, por exemplo, a paralisação de serviços públicos ou privados essenciais, como a rede de saúde, em um país combalido pelos efeitos nefastos da pandemia.

O perigo real e imediato do *ransomware* em território nacional exige, com urgência, o aprimoramento tecnológico das ferramentas de investigação digital forense e a capacitação dos membros do Ministério Público Nacional, das forças policiais e do Poder Judiciário, no âmbito de uma estratégia coordenada de enfrentamento e resposta aos crimes cibernéticos. É inegável que o combate aos crimes cibernéticos não poderá ser realizado sem a parceria com as inovações do setor privado, na esfera de segurança da informação e defesa de infraestruturas críticas. A eficiência e a celeridade na construção conjunta de um novo modelo de investigação de cunho repressivo, aliado ao desenvolvimento e à divulgação de medidas preventivas e de inteligência, provavelmente fomentará que as vítimas não cedam às chantagens do sequestro criptográfico de dados e, assim, desestimula-se o uso de *ransomware* como meio para execução de crimes graves.

Há um quarto de século, o atual cenário cibernético catastrófico havia sido previsto pelos pesquisadores da Universidade de Columbia, os quais foram desprezados ou ridicularizados como teóricos da conspiração. É inadmissível que os operadores do sistema jurídico-penal brasileiro permaneçam em *berço esplêndido*, assistindo, impávidos, à explosão da criminalidade cibernética em território pátrio, que cresce, exponencialmente, graças à globalização dos meios de comunicação e à expansão de grupos ocultos no que convencionou denominar de *darkweb*. A somar-se a esse quadro, há necessidade de reorganização legislativa dos tipos penais de crimes cibernéticos e dos meios de coleta e produção de provas digitais, adequando-os à realidade nacional. Igualmente,

urge reorganizar os órgãos integrantes do sistema jurídico-penal para que as atividades funcionais sejam o reflexo de modelos orientados em inteligência de ameaças cibernéticas. Por derradeiro, os órgãos públicos, sobretudo o Ministério Público Nacional, espelhando-se no que está a ocorrer no setor privado, nesse exato momento, devem rever as arquiteturas de redes, as organizações de serviços e os meios de prevenção, detecção, análise e resposta aos incidentes cibernéticos, haja vista a migração não planejada para novos meios de conexão e operação de atividades em *home office*, que ampliaram, nos últimos meses, as superfícies de ataques e os pontos de vulnerabilidades.

7. Referências

AMORIM, Felipe. Ataque hacker ao TSE também acessou dados de 2020 do tribunal. *UOL*, 2020. Disponível em: <https://noticias.uol.com.br/eleicoes/2020/11/19/ataque-hacker-ao-tse-tambem-acessou-dados-de-2020-do-tribunal.htm>. Acesso em: 6 mar. 2021.

BERR, Jonathan. "WannaCry" ransomware attack losses could reach $4 billion. *CBS NEWS*, 16 maio 2017. Disponível em: <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>. Acesso em: 28 fev. 2021.

BERTOLLI, Emilia. O criptowall em 2018. *Varonis*, 5 jul. 2018. Disponível em: <https://blog.varonis.com.br/o-cryptowall-em-2018/>. Acesso em: 28 fev. 2021.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal*: Parte Geral. 8 ed. São Paulo: Saraiva, 2003.

BULLETIN board system. In: *WIKIPÉDIA*: a enciclopédia livre. Wikimedia, 2021. Disponível em: <https://pt.wikipedia.org/wiki/Bulletin_board_system>. Acesso em: 3 mar. 2021.

CISA. *Cybersecurity & Infrastructure Security Agency*. Disponível em: <https://www.cisa.gov/about-cisa>. Acesso em: 28 fev. 2021.

DUCKLIN, Paul. "Locky" ransomware: O que você precisa saber. *Naked Security*, 17 fev. 2016. Disponível em: <https://nakedsecurity.sophos.com/pt/2016/02/17/locky-ransomware-what-you-need-to-know/>. Acesso em: 28 fev. 2021.

ESCOSTEGUY, Diego. Hacker criptografou todos os processos e emails do STJ. *O Bastidor*, 5 nov. 2020c. Disponível em: <https://obastidor.com.br/justica/hacker-criptografou-todos-os-processos-e-emails-do-stj-19>. Acesso em: 2 mar. 2021.

ESCOSTEGUY, Diego. CNJ, Governo de Brasília e SUS sofrem ataque semelhante ao do STJ. *O Bastidor*, 5 nov. 2020a. Disponível em: <https://obastidor.com.br/investigacao/cnj-governo-de-brasilia-e-sus-sofrem-ataque-semelhante-ao-do-stj-25>. Acesso em: 2 mar. 2021.

ESCOSTEGUY, Diego. Hacker cobra resgate de dados sequestrados do STJ. *O Bastidor*, 5 nov. 2020b. Disponível em: <https://obastidor.com.br/justica/hacker-cobra-resgate-de-dados-sequestrados-do-stj-26>. Acesso em: 2 mar. 2021.

ESCOSTEGUY, Diego. Técnico responsável pelo firewall do STJ trabalhava de casa. *O Bastidor*, 5 nov. 2020d. Disponível em: <https://obastidor.com.br/justica/tecnico-responsavel-pelo-firewall-do-stj-trabalhava-de-casa-23>. Acesso em: 2 mar. 2021.

SMYTH, Chris. EVERY hospital tested for cybersecurity has failed. *The Times*, 2018. Disponível em: <https://www.thetimes.co.uk/article/every-hospital-tested-for-cybersecurity-has-failed-97vc6rqkq>. Acesso em: 28 fev. 2021.

FISCUTEAN, Andrada. *A history of ransomware*: The motives and methods behind these evolving attacks. *CSO Online*, 27 jul. 2020. Disponível em: <https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html?page=2>. Acesso em: 3 mar. 2021.

Global cyberattack strikes dozens of countries, cripples U.K. hospitals. *CBS News*, 12 maio 2017. Disponível em: <https://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack/>. Acesso em: 28 fev. 2021.

GREENBERG, Andy. *Sandworm*: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday, 2019.

GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, 22 ago. 2018. Disponível em: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>. Acesso em: 3 mar. 2021.

GROOT, Juliana. A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. *Digital Guardian*, 2020.

HOSPELHORN, Sarah. What is The Cyber Kill Chain and How to Use it Effectively. *Varonis*, 29 mar. 2020. Disponível em: <https://www.varonis.com/blog/cyber-kill-chain/>. Acesso em: 2 mar. 2021.

JOYCE, Sandra. Ransomware: The Threat We Can No Longer Afford to Ignore. *FireEye*, 29 out. 2020. Disponível em: <https://www.fireeye.com/blog/executive-perspective/2020/10/ransomware-the-threat-we-can-no-longer-afford-to-ignore.html>. Acesso em: 28 fev. 2021.

KELION, Leo. Cryptolocker ransomware has 'infected about 250,000 Pcs'. *BBC*, 24 dez. 2013. Disponível em: <https://www.bbc.com/news/technology-25506020?tblang=english>. Acesso em: 28 fev. 2021.

LARSON, Selena. Massive cyberattack targeting 99 countries causes sweeping havoc. *CNN Business*, 13 maio 2017. Disponível em: <https://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/>. Acesso em: 28 fev. 2021.

LUCHETE, Felipe; GALLI, Marcelo. Dez tribunais tiram site do ar após ataque cibernético mundial. *Consultor Jurídico*, 12 maio 2017. Disponível em: <https://www.conjur.com.br/2017-mai-12/dez-tribunais-tiram-site-ar-ataque-cibernetico-mundial>. Acesso em: 2 mar. 2021.

MCKENZIE, Lindsay. Cyberextortion Threat Evolves. *Inside Higher Ed*, 11 jun. 2020. Disponível em: <https://www.insidehighered.com/news/2020/06/11/colleges-face-evolving-cyber-extortion-threat>. Acesso em: 2 mar. 2021.

MOIR, Robert. Defining Malware: FAQ. *Microsoft*, 2009. Disponível em: <https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN>. Acesso em 28 fev. 2021.

O'NEILL, Patrick Howell. A patient has died after ransomware hackers hit a German hospital. *Technology Review*, 18 set. 2020. Disponível em: <https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/>. Acesso em: 28 fev. 2021.

RADIN, Andrew. *Hybrid Warfare in the Baltics*: Threats and Potential Responses. California: Rand Corporation, 2017.

RANSOMWARE - definition, prevention and removal. *Kaspersky*. Disponível em: <https://www.kaspersky.com/resource-center/threats/ransomware>. Acesso em: 28 fev. 2021.

ROOTKIT: What is a Rootkit?. *Veracode*. Disponível em: <veracode.com/security/rootkit>. Acesso em: 28 fev. 2021.

ROSENCRANCE, Linda. Advanced Persistent Threat (APT). *Tech Target*, 2020. Disponível em: <https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT>. Acesso em: 2 mar. 2021.

SAISSE, Renal Cabral. Ransomware: "sequestro" de dados e extorsão digital. *Direito & TI*, 2016. Disponível em: <http://direitoeti.com.br/artigos/ransomware-sequestro-de-dados-e-extorsao-digital/>. Acesso em: 2 mar. 2021.

SHARMAN, Jon. Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France. *Independent*, 13 maio 2017. Disponível em: <https://www.independent.co.uk/news/uk/home-news/nissan-sunderland-cyber-attack-ransomware-nhs-malware-wannacry-car-factory-a7733936.html>. Acesso em: 28 fev. 2021.

SINGLETON, Camille; KIEFER, Christopher. VILLADSEN, Ole. Ransomware 2020: Attack Trends Affecting Organizations Worldwide. *Security Intelligence*, 28 set. 2020. Disponível em: <https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/>. Acesso em: 2 mar. 2021.

Spear Phishers: Angling To Steal Your Financial Info. *The FBI – Federal Bureau of Investigation*, 2009. Disponível em: <https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109>. Acesso em: 3 mar. 2021.

STAFF, Dice. Cybersecurity in 2021: 5 Trends Security Pros Need to Know. *Dice*, 14 dez. 2020. Disponível em: <https://insights.dice.com/2020/12/14/cybersecurity-in-2021-5-trends-security-pros-need-to-know/>. Acesso em: 2 mar. 2021.

The State of Ransomware 2020: Results of an independent study of 5,000 IT managers across 26 countries. *Sophos*, 2020. Disponível em: <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>. Acesso em: 2 mar. 2021.

TROJAN.TeslaCrypt. *F-Secure*. Disponível em: <https://www.f-secure.com/v-descs/trojan_teslacrypt.shtml>. Acesso em: 28 fev. 2021.

VICHI, Leonardo Perin. *Inteligência Cibernética e a Linguística Forense como Ferramenta*: o uso da análise linguística para atribuição de autoria em ciberataques. *Núcleo de Estudos Estratégicos em Defesa e Segurança da UFSCAR*, 2021. Disponível em: <http://needs.df.ufscar.br/artigos_de_opiniao3/127/leonardo_perin_vichi:_inteligencia_cibernetica_e_a_linguistica_forense_como_ferramenta_-_o_uso_da_analise_linguistica_para_atribuicao_de_autoria_em_ciberataques>. Acesso em: 21 jul. 2021.

VIJAVAN, Jai. Ransomware Attacks Show Little Sign of Slowing in 2021. *DARK Reading*, 20 out. 2020. Disponível em: <https://www.darkreading.com/attacks-breaches/ransomware-attacks-show-little-sign-of-slowing-in-2021/d/d-id/1339231>. Acesso em: 2 mar. 2021.

VILLADIEGO, Ricardo. Attacker Dwell Time: Ransomware's Most Important Metric. *DARK Reading*, 2020. Disponível em: <https://www.darkreading.com/risk/attacker-dwell-time-ransomwares-most-important-metric/a/d-id/1338978>. Acesso em: 2 mar. 2021.

WOOD, Collin. University of Utah pays ransomware attackers $457K. *ED Scoop*, 21 ago. 2020. Disponível em: <https://edscoop.com/university-utah-pays-ransomware-attackers-457k/>. Acesso em: 2 mar. 2021.

YOUNG, Adam; YUNG, Moti. *Cryptovirology*: Extortion-Based Security Threats and Countermeasures. Article published in the Proceedings of 1996 IEEE Symposium on Security and Privacy. May 6-8. Copyright 1996 IEEE. Disponível em: <https://www.researchgate.net/publication/2301959_Cryptovirology_Extortion-Based_Security_Threats_and_Countermeasures>. Acesso em: 2 mar. 2021.

YOUNG, Adam; YUNG, Moti. Cryptovirology: The Birth, Neglect, and Explosion of Ransomware. *Communications of the ACM*, 2017. Disponível em: <https://cacm.acm.org/magazines/2017/7/218875-cryptovirology/fulltext>. Acesso em: 3 mar. 2021.

YOUNG, Adam; YUNG, Moti. *Malicious Cryptography Exposing Cryptovirology*. Indiana: Wiley Publishing Inc., 2004.

2020 Cyber Threats Report. Netwrix, 2020. Disponível em: <https://www.netwrix.com/2020_cyber_threats_report.html>. Acesso em: 28 fev. 2021.

RENATO TEIXEIRA REZENDE

Promotor de Justiça do Ministério Público do Estado de Minas Gerais.