A Inteligência Artificial e *Malware*

O *malware* é ameaça constante na vida dos profissionais da Ciência da Computação[1]. Em regra, além de atrasarem projetos de sistemas devido ao tempo dispensado para criação de barreiras contra os cibercriminosos que os criam, também exige que os profissionais mantenham total vigilância da vida do sistema operacional, para que um *malware* não consiga romper o exército de combate previamente constituído.

O poder de invasão do *malware* se assemelham, de modo análogo, ao modo como agem os criminosos que cometem os crimes tradicionais contra o patrimônio. Para serem combatidos, previamente são construídas grades, colocados alarmes e cerca elétrica, bem como há monitoramento, de modo a garantir a segurança das casas contra diversos tipos penais, seja o furto, seja roubo, seja o sequestro, entre outros. O *malware* se manifesta de diversas formas, sendo elas:

---

[1] *Malware* ou "software malicioso" é um termo mais amplo que descreve qualquer programa ou código malicioso que seja prejudicial aos sistemas. Hostil, intrusivo e intencionalmente prejudicial, o malware invade, danifica ou desabilita computadores, sistemas de computador, redes, tablets e dispositivos móveis, geralmente assumindo o controle parcial das operações de um dispositivo. Assim como a gripe para os humanos, ele interfere no funcionamento normal. Malware é uma maneira de ganhar dinheiro à sua custa de forma ilícita. Embora malware não possa danificar o hardware físico dos sistemas e equipamentos de rede (com uma exceção conhecida— consulte a seção Google Android abaixo), ele pode roubar, criptografar ou excluir seus dados, alterar ou sequestrar funções essenciais do computador e espionar a atividade de seu computador sem seu conhecimento ou permissão. *Malware* é um vírus? Sim e não. Embora todos os vírus de computador sejam *malware*, nem todo *malware* é um vírus. Os vírus são apenas um tipo de *malware*. Muitas pessoas usam os dois termos de forma intercambiável, mas do ponto de vista técnico, vírus e malware não são a mesma coisa. De outra maneira, *malware* é um código malicioso. Vírus de computador são códigos maliciosos que se espalham por computadores e redes. (BELCIC, Ivan. O que é malware? *In*: Avast. [S.I.], 28 de setembro de 2019. Disponível em: https://www.avast.com/pt-br/c-malware. Acesso em: 30 jun. 2020). O termo *malware* é uma contração das palavras inglesas *malicious software* (software malicioso, em tradução livre). Simplificando, *malware* é qualquer parte de um software que tenha sido codificada com o objetivo de danificar dispositivos, roubar dados e causar danos às pessoas. Vírus, cavalos de Tróia, spywares e ransomwares estão entre os diferentes tipos de *malwares*. Frequentemente um *malware* é desenvolvido por times de hackers que, na maioria das vezes, estão apenas buscando uma forma de fazer dinheiro, seja pela proliferação do próprio *malware* ou por meio de leilão na Dark Web. De qualquer forma, pode haver outras razões para a criação de malwares. Esses softwares maliciosos podem ser usados como ferramentas de protesto, uma forma para testar a segurança de uma rede ou até mesmo como armas de guerra entre governos. Mas não interessa o motivo ou como um *malware* surge, é sempre uma notícia ruim quando ele acaba invadindo o seu PC. (REGAN, Joseph. O que é malware? Como malwares funcionam e como se livrar deles. *In*: AVG. [S.I.], 10 DE JULHO DE 2019. Disponível em: https://www.avg.com/pt/signal/what-is-malware. Acesso em: 28 jun. 2020). MALWAREBYTES. **Tudo sobre malware**. *In*: Malwarebytes. Cork, Irlanda, [2020?]. Disponível em: https://br.malwarebytes.com/malware/. Acesso: 30 jun. 2020.

(i) *Vírus*: pode ser considerado o *malware* mais popular; as pessoas costumam afirmar: *"tive que formatar meu computador, um vírus travou minha máquina"*. Em regra, o vírus busca se anexar noutro programa e, ao se autoexecutar, dá indicativos de sua presença diante de redução considerável na velocidade de *hardware*, que deixa morosos os programas na máquina instalados, alterando os códigos dos programas;

(ii) *Worms*: muito semelhante ao vírus, esse *malware* se multiplica com o objetivo de se proliferarem na rede para atingirem outros computadores. Além do dano de alterar os códigos dos programas, também destroem dados e arquivos;

(iii) *Spyware*: caracteriza-se pela transparência; é um *malware* que a maioria dos usuários sequer notam sua presença no sistema operacional. Seu objetivo é observar todas as atividades do usuário e repassá-las ao autor do *software*;

(iv) *Ransomware*: o *malware* que paralisa o dispositivo ainda tem a capacidade de criptografar seus arquivos. Todo esse potencial danoso com o intuito pedir uma recompensa nos crimes contra o patrimônio tradicionais poderia equipará-lo à extorsão mediante sequestro. O *ransoware* é considerado um *malware* lucrativo para os cibercriminosos, porque exige um pagamento rápido a ser realizado pelo usuário. Em regra, mediante transferência de criptomoedas que, por meio da blockchain, não deixam rastros no caminho do valor de recompensa até a chave pública do cibercriminoso. O caminho para se alcançar o procedimento e o código do *ransomware* é tarefa fácil na *web deep*; porém, livrar-se dele é tarefa árdua.

(v) *Trojan*: mais conhecido como cavalo de Tróia, é um *malware* extremamente danoso ao sistema operacional[2]. Ele age com a

[2] - Oi! Eu sou um *hacker* que tem acesso ao seu sistema operacional. Também tenho total acesso à sua conta. Seu IP atual: 200.147.36.29. Eu já venho te observando há alguns meses. O que eu vim te falar é que seu computador foi infectado com um malware em um site adulto que você visitou. Caso você não saiba como isso funciona, eu vou explicar. O Vírus Trojan me dá total acesso e controle de um computador, celular ou de algum outro dispositivo. Isso significa que eu posso ver tudo que está na sua tela, posso ativar sua câmera e o microfone, mas isso tudo sem você saber. Eu também tenho acesso a todos os seus contatos e todas as suas mensagens.

estratégia de conduzir o usuário ao erro. Quando penetrado no ambiente, os cibercriminosos que comandam o *malware* furtam as informações financeiras do usuário e, muitas vezes, deixam rastros ao instalarem o *vírus* e *ransomware*.

(vi) *Adware*: o *malware* é um *software* indesejado criado para inserir anúncios na tela do navegador da *Web* do usuário. Em regra, disfarça-se como legítimo ou se aparenta sobre outro programa, de modo a instalar-se no sistema operacional, seja dos computadores, seja dos *smartphones*;

(vii) Keylogger: esse *malware* registra a ordem de pressionamento de tecla do usuário, e as envia ao cibercriminoso, que seleciona apenas as informações de nome de usuário, senhas ou detalhes de cartões de crédito;

(viii) *Exploits*: é um *malware* que se utiliza dos *bugs* e vulnerabilidades do sistema para que o cibercriminoso assuma o controle da máquina. O *malware* também se mostra por meio das propagandas maliciosas que atacam por meio de sites legítimos; os usuários que pensam estar acessando conteúdos legítimos. Quando o usuário acessa o conteúdo aparentemente legítimo, o cibercriminoso lança o seu *malware*, em um *download drive-by,* e se instala no computador do usuário;

(ix) *Rootkit*: nesse *malware,* o cibercrimonoso adquire a administração do sistema infectado, mantendo-se escondido do próprio usuário, driblando o sistema operacional e o *software* do sistema;

Você deve estar pensando: por que meu antivírus não detectou o malware? Resposta: Meu malware usa o driver, eu atualizo suas assinaturas a cada 4 horas para que seu antivírus não o detecte. Eu gravei um vídeo mostrando como você obtém prazer na metade esquerda da tela, e na metade direita é possível ver o vídeo que você estava assistindo. Com apenas um clique eu posso enviar esse vídeo para todos os seus contatos de e-mails e para seus amigos nas redes sociais. Eu também posso liberar o acesso a todos os seus e-mails e mensagens. Caso queira evitar isso, transfira a quantia de 500 dólares americanos para a minha carteira de bitcoin (se você não sabe como fazer isso, pesquise no Google: "Comprar Bitcoin"). Meu endereço do *bitcoin* (Carteira BTC) é: 13LjWUqvyvGGLmYyoGGCVvAmaNbLzx8wpw. Depois que eu receber o pagamento, vou apagar o vídeo e você nunca mais vai ouvir falar de mim. Eu dou a você 50 horas (mais de 2 dias) para fazer o pagamento. Essa mensagem tem um aviso de leitura, então o temporizador vai começar a contar quando você ver essa mensagem. Fazer uma denúncia em algum lugar não faz sentido, porque esse e-mail não pode ser rastreado, nem o meu endereço bitcoin. Eu não cometo erros. Se eu descobrir que você compartilhou essa mensagem com outra pessoa, o vídeo será imediatamente enviado a todos os seus contatos. Saudações!

(x) *Mineração maliciosa de criptomoeda*: denominada também de *cryptojacking,* é um *malware* em ascensão, usualmente como já visto, utilizado pelo cavalo de Tróia para exigir a recompensa de criptomoedas. O *malware* utiliza o poder de *hardware* da máquina invadida para minerar criptomoedas. Desse modo, diminui substancialmente a capacidade de *hardware* da máquina do usuário, e as criptomoedas mineiradas vão diretamente para a *hash* do cibercriminoso.

A ameaça do *malware* está presente na história da computação desde a sua criação e, enquanto descrevo isso, cibercriminosos acabam de invadir as contas do *Twiter* de Jeff Bezos, Bill Gates, Elon Musk e Barack Obama, para solicitar, de seus seguidores, o depósito em *hashs* públicas de carteiras privadas que jamais saberemos os seus proprietários. E notem: a característica do *modus operandi* do cibercriminoso desse caso concreto não se enquadra a nenhum dos *malwares* descritos anteriormente, o que faz resultar noutra espécie de cibercrime. Destaca-se, desse modo, que a diferença da tecnologia do início da computação para a atual tecnologia é esta: tempos atrás, eram localizados os IP da máquina do cibercriminoso que enviavam o *malware*. Atualmente, não se pode localizar a conta de criptomoeda que recebeu milhões de dólares em segundos após a postagem *fake* no *Twitter* das personalidades, e talvez jamais será localizada.

Historicamente, o primeiro vírus reconhecido e documentado exsurgiu no decorrer da década de 1970. Destaca-se Bob Thomas, o criador do cartão de visita *Creeper, que disse: "Eu sou a trepadeira, me pegue se puder!"*. Ele desenvolveu um *malware* inofensivo, com o intuito de demonstrar à comunidade da ciência da computação a capacidade de um *software* ser transmitido automaticamente de um computador para outro.[3] A motivação de Bob Thomas

[3] Era 1971, e essa mensagem começou a aparecer diante dos olhos atônitos dos poucos usuários que lidavam com os computadores que faziam parte da ARPANET (a rede original que, com o passar do tempo, daria origem à Internet). O que essa frase enigmática significava? Este foi o cartão de visita do Creeper, o primeiro vírus de computador da história, desenvolvido por Bob Thomas, programador da BBN Technologies. Embora sua mensagem fosse desconcertante, a intenção de Thomas não era prejudicial. Seu objetivo era criar um programa para confirmar, na prática, se isso poderia ser movido entre computadores. E ele conseguiu isso. No entanto, o Creeper era totalmente inofensivo e não tinha nada a ver com os vírus nocivos que se desenvolveram anos depois. Depois de "infectar um computador", o Creeper exibia sua

foi uma extensão das ideias de John von Neumann na década de 1940, que acabou criando o primeiro antivírus da história, denominado *Reaper*, o "*podador*".[4]

Muitos especialistas da computação afirmam que o *Creeper* não tinha um caráter de contaminação potencial, em virtude da sua incapacidade de se multiplicar. Porém, sabe-se que essa não era sua função central, e, sim, de vagar de um computador para outro. Por isso, é verdadeiro afirmar que o *Creeper* foi o primeiro antivírus, muito embora, na época, não existisse a expressão antivírus figurando na Ciência da Computação.

Porém, aqueles que não reconheciam o *Creeper* como um *malware* real, diante da sua ausência de ofensividade, exsurgiria logo em seguida um *malware* de caráter robusto e com tamanha gama de ofensividade, denominado *Rabbit*. O *malware* verdadeiramente ofensivo, diferentemente da característica do *Creeper*, acabava invadindo o sistema e causando sua falha. Logo depois, no início da década de 80, sucedeu-se o *malware Elk Cloner*. Este atingiu o Apple II, um sistema operacional iOS, já destacado na época pela sua segurança. Por meio de disquetes de inicialização do sistema operacional, acabou encontrando uma porta de entrada.

No final da década de 80, foi criado o primeiro *malware* de computador, chamado de *Brain*. Esse vírus foi propagado em massa, infectando aproximadamente 20.000 máquinas. Isso ocorreu por meio da cópia pirata do MS-DOS,[5] com intuito de controlá-los a obstar a disseminação no computador

---

mensagem, começava a imprimir um arquivo e, antes que a impressão terminasse, passava para o próximo computador na rede, desaparecendo do primeiro. Embora seu mecanismo possa parecer muito simples, é importante ter em mente que foi a primeira vez que o *software* capaz de ser transmitido automaticamente de um computador para outro foi criado. THE CREEPER Worm, the first computer vírus. *In*: HISTORY OF INFORMATION.com. [S.I.], [2020?]. Disponível em: http://www.historyofinformation.com/detail.php?entryid=2860. Acesso em: 16 jul. 2020.

[4] Não há registros confiáveis sobre quem desenvolveu o Reaper. Algumas versões afirmam que era o próprio Bob Thomas, enquanto outras afirmam que foi obra de Ray Tomlinson, o famoso criador de e-mail. A verdade é que o Reaper foi muito eficaz em seu objetivo: assim que detectou o ataque do Creeper, ele o removeu do sistema, impedindo que ele se espalhasse para outros computadores. HISTORY of computer viroses. Creeper and Reaper. *In*: PANDORAFMS: Monitoring Blog. [S.I.], 10 de outubro de 2018. Disponível em: https://pandorafms.com/blog/creeper-and-reaper/. Acesso em: 16 jul. 2020.

[5] O sistema operacional MS-DOS é responsável pela comunicação entre o usuário e o computador, recebendo ordens do usuário e enviando as respostas através do vídeo. Para que haja esta comunicação, o DOS utiliza uma linguagem própria denominada linguagem de controle. É um sistema mono-usuário e com memória real, isto é só pode ser usado por um usuário de cada vez e só podem ser executados programas que caibam na memória. Quando o computador é ligado, após serem executadas as instruções contidas na memória ROM, começa a procura pelo Sistema Operacional. Se for executado o sistema operacional MS-DOS, o computador

do usuário sem autorização. O vírus enviava uma singela mensagem para entrar em contato com o fabricante do MS-DOS.

Disso, resulta afirmar que, desde os primórdios civilizatórios da Ciência da Computação, os cibercriminosos estruturaram uma indústria de *malware*. Desde então, os sistemas computacionais passaram cada vez mais a dedicar tempo e dinheiro em busca de uma verdadeira luta contra os *malwares*. Isso se tornou um ciclo autopoético que se retroalimenta; quer dizer, quanto mais os *experts* criam barreiras e melhoram suas defesas anti-malwares, os cibercriminosos se desenvolvem, criando modos de aparição. Um exemplo disso é a recente invasão no *Twitter* de personalidades mundiais, exigindo um *cryptojacking* de recompensa.

Atualmente, com a ascensão da internet das coisas (Iot),[6] a área de atuação dos cibercriminosos aumentou de modo inimaginável, em virtude das oportunidades oferecidas pela avalanche tecnológica. Ou seja, a comunicabilidade – transmissão de dados – entre os dispositivos móveis[7] torna-

---

passa a executar as instruções contidas nesse programa. E, para comunicar ao usuário que toda a operação até então executada teve bom êxito e que o computador está pronto para ser usado, é apresentado na tela do vídeo o *prompt* (mensagem inicial do ms-dos), o qual indica qual é o drive corrente (em que drive está se trabalhando). Todas as informações que são armazenadas nos discos ficam gravadas dentro de "arquivos". E para que seja possível identificar cada um dos arquivos gravados em um disco, cada um deles deve possuir um nome. O MS-DOS aceita até 8 caracteres no nome do arquivo e permite também a utilização de uma extensão com até 3 caracteres, a qual serve para identificar o tipo de arquivo. Para separar o nome do arquivo de sua extensão deve-se colocar um ponto (.) entre eles. UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC). **Sistema Operacional MS-DOS**. Santa Catarina: UFSC, Departamento de Informática e Estatística, [2020?]. Disponível em: http://www.inf.ufsc.br/~j.barreto/cca/sisop/msdos.html. Acesso: 19 jul. 2020.

[6] O conceito de Internet das Coisas (IoT) foi introduzido por Kelvin Ashton em 1999 como resultado de sua pesquisa para utilizar etiquetas eletrônicas RFID na cadeia de produção. Adicionalmente, foi introduzida a utilização de sensores e atuadores, apesar de suas restrições de energia, processamento e memória. Com o avanço da microeletrônica, os preços das interfaces de redes diminuíram, e seu tamanho físico também, viabilizando a introdução de telecomunicações nesses objetos, tornando-os assim “Objetos Inteligentes e Conectados”. Dessa maneira, a INTERNET globalizada passou a incorporar os objetos inteligentes, surgindo assim a Internet das Coisas. (ASHTON, Kevin. Internet das Coisas, nova revolução da conectividade. Entrevista cedida à Inovação em Pauta. **Inovação em Pauta**, Porto Alegre, n. 18, p. 6-9, 14 dez. 2014. Disponível em: http://www.flip3d.com.br/web/pub/finep/. Acesso em; 28 de abr. 2019). Vasseur e Dunkels, afirmam que para que a Internet das Coisas exista faz-se necessário a utilização dos objetos inteligentes, que por definição é um objeto equipado com uma forma de sensor, um pequeno microprocessador, um dispositivo de comunicação, e uma fonte de energia. VASSEUR, J. P.; DUNKELS, A. **Interconnecting Smart Objects with IP**. Burlington, EUA: Morgan Kaufmann Publishers, 2010.

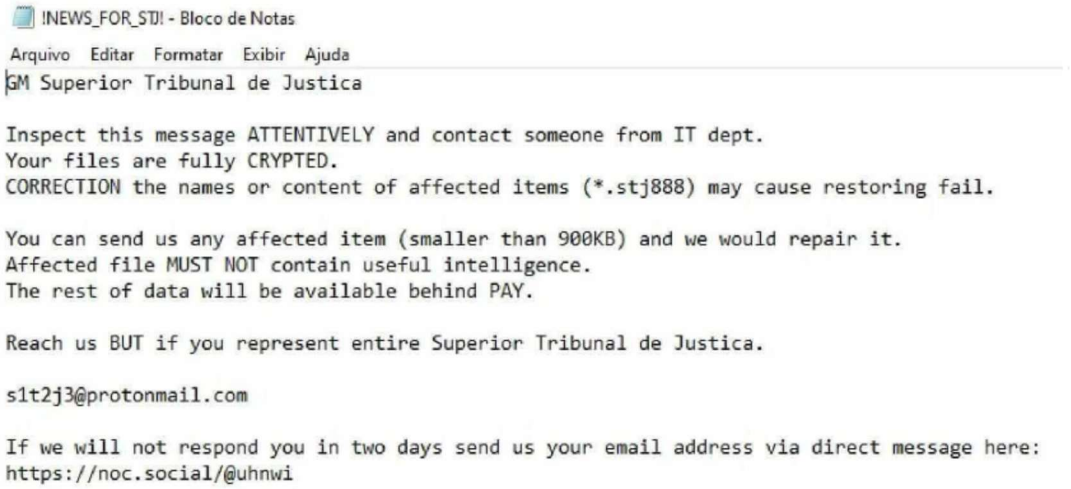
[7] Conforme a Symantec, os malwares para dispositivos móveis aumentaram 54% em 2017, enquanto ataques de IoT teve um aumento de 600%. SYMANTEC. **Executive Sumary**. 2018 Internet Security Threat Report, v. 23, mar. 2018. Disponível em: https://docs.broadcom.com/doc/istr-23-2018-executive-summary-en-aa. Acesso em: 21 nov. 2020.

se alimento para que se procriem *malwares* inteligentes e sofisticados. Como se viu anteriormente, atualmente, há *malwares* que se utilizam da criptografia para invadir os sistemas operacionais. A exemplos, os cavalos de Tróia disponíveis na *deep web*: para que cibercriminosos invadam os sistemas operacionais alheios e passem a exigir pagamentos em criptomoedas, os *ransomwares* passaram a ser notícias rotineiras nos sistemas computacionais pelo mundo.

Recentemente, o Superior Tribunal de Justiça sofreu um ataque de *ransomware*, mais conhecido como *RansomExx*, que já afetou órgãos como o Departamento de Transporte do Texas e empresas como a IPG Photonics, que desenvolve *lasers* para uso médico e industrial, além de canhões laser para as forças armadas dos Estados Unidos. O objetivo do *RansomExx* é invadir a rede da vítima para acessar os dados privados sem criptografia e se espalhar para outros sistemas internos; assim, se infiltrar no controlador de domínio do *Windows* para distribuir os arquivos de *ransomware* e criptografar arquivos em toda a rede.

O site *O Bastidor* publicou uma captura de um arquivo de texto em que o invasor dá as orientações sobre como contatá-lo para combinar o pagamento para que os arquivos sejam liberados.[8]

Figura 9 – *Ransomware*



[8] BRITO, Paulo. STJ: mais de 1.200 servidores congelados, backups destruídos. *In*: CISO Advisor. [S.l.], 05 de novembro de 2020. Diponível em: https://www.cisoadvisor.com.br/stj-mais-de-1200-servidores-congelados-backups-destruidos/. Acesso em: 15 nov. 2020.

Fonte: Escosteguy (2020)[9]

Em virtude dessas considerações, reconhece-se que a evolução tecnológica é notoriamente disruptiva. Com efeito, disruptiva também é a capacidade do *malware* de se moldar a tal evolução; tornou-se um jogo de caça e caçador. No caminho da internet das coisas, o *botnet Mirai* e suas inúmeras variâncias é uma “pedra no sapato” no caminho do avanço tecnológico. O Mirai é outro *malware* inteligente e sofisticado. Ele infecta os dispositivos inteligentes executados em processadores ARC,[10] que acabam por transformar os dispositivos numa rede de *bots*; são definidos como verdadeiros zumbis controlados remotamente que iniciam os ataques DDoS.[11]

Nesse sentido, com a abrangência do espectro do *malware* em torno da inteligência artificial, muitos dos indivíduos tendem a acreditar que esse avanço

---

[9] ESCOSTEGUY, Diego. Hacker do STJ deixou hashtag “estupro culposo” no sistema do tribunal. *In*: O BASTIDOR. [S.I.], 05 de novembro de 2020. Disponível em: https://obastidor.com.br/justica/hacker-do-stj-deixou-hashtag-estupro-culposo-no-sistema-do-tribunal-22. Acesso em: 16 nov. 2020.

[10] O conjunto de instruções ARC têm 32 registradores de 32 bits de uso geral, um PC e um IR. Um registrador de status da ULA (PSR), o qual contém informações (bits flags) os quais informam o resultado da operação aritmética realizada, tais como, zero, overflow, carry e outras. Todas as instruções têm o tamanho de 32 bits. As operações com a memória são feitas usando as instruções Load e Store. As operações aritméticas são realizadas entre registradores e o resultado é armazenado em registrador. São aproximadamente 200 instruções para o SPARC e o ARC se baseou com um sub-conjunto de 15 instruções. Cada instrução é representada por um mnemônico, que é o nome que representa a instrução. MURDOCCA, Miles J.; HEURING, Vincent P. **Introdução à Arquitetura de Computadores**. Rio de Janeiro: Editora Campus, 2010.

[11] Os ataques de rede distribuídos muitas vezes são chamados de ataques de negação de serviço distribuído (DDoS), primeira interação consiste justamente na criação de uma rede de máquinas comprometidas, também chamada de botnet. Esse tipo de ataque aproveita os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa. Os bots são executados em grupos de zombies que são controlados remotamente por atacantes. O ataque DDoS envia múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto. (KOLIAS, Constantinos *et al*. DDoS in the IoT: Mirai and other botnets. **Computer**, v. 50, n. 7, p. 80-84, dez. 2016. Disponível em: https://www.researchgate.net/publication/318288727_DDoS_in_the_IoT_Mirai_and_other_botnets. Acesso em: 12 nov. 2019). Os recursos de rede, como servidores Web, conseguem atender a um limite finito de solicitações simultaneamente. Além do limite de capacidade do servidor, o canal que conecta o servidor à Internet também tem largura de banda/capacidade finita. Sempre que o número de solicitações excede os limites de capacidade de qualquer componente da infraestrutura, o nível do serviço tende a sofrer de uma das seguintes maneiras: i) A resposta às solicitações é muito mais lenta do que o normal. ii) Algumas ou todas as solicitações dos usuários podem ser totalmente ignoradas. Em geral, o objetivo final do invasor é impedir totalmente o funcionamento do recurso da Web, ou seja, uma "negação de serviço" total. O invasor também pode solicitar um pagamento para interromper o ataque. Em certos casos, um ataque DDoS pode até ser uma tentativa de desacreditar ou prejudicar os negócios de um concorrente. ZHU, Z. *et al*. Botnet research survey. *In*: ANNUAL COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE, 38., 2004. **XXXVIII Annual**… Los Alamitos, CA, USA: IEEE Computer Society, 2004. p. 967–972.

tecnológico pode ser o caminho para solucionar os desafios de segurança cibernética. Contudo, do mesmo modo, uma grande parcela dos pesquisadores da ciência da computação concorda que as discussões sobre a implementação da IA deve ser aliada a uma infraestrutura defensiva. A luta entre analistas de segurança e desenvolvedores de *malware* é uma batalha sem fim, aliada ainda à complexidade de os cibercriminosos cambiarem seus ataques tão rapidamente quanto ao crescimento tecnológico.

Destaca-se o valor imensurável da IA como ferramenta na luta contra os cibercriminosos. Por isso, convém destacar a importância dos projetos de IA abarcarem proteções contra *malware*. Especialmente, se um projeto de IA sofrer o ataque por razões financeiras que acabam motivando o cibercriminoso a dedicar o tempo necessário para contornar os algoritmos de proteção do *machine learning,*[12] assim, a construção da inteligência artificial pode estar comprometida diante da possibilidade de invasão de um *malware*.

Em maio de 2017, uma avançada ferramenta de invasão a sistemas de informática desenvolvida pela *Equation Group*, criada por um grupo de *hackers* operados de dentro da Agência de Segurança Nacional dos Estados Unidos, propagou arquivos de exploração, denominados de *The Shadow Brokers,* por milhares de computadores ao redor do mundo. As máquinas infectadas tornaram-se “reféns” de um sistema de controle central comandado por indivíduos mal-intencionados que obtiveram acesso à ferramenta após o vazamento de seu código-fonte. Logo a seguir, o grupo de *hackers* passaram a realizar um leilão *on-line* dos dados furtados virtualmente.

Inicialmente, o cibercrime ocorreu no Brasil explorando a vulnerabilidade do sistema Windows, que bloqueou o acesso do usuário a seus arquivos contidos no *explorer*. O acesso, após a invasão, passaria então a ser liberado somente após o pagamento de uma espécie de resgate. Esse crime foi denominado de *Wannacry*.[13]

---

[12] O aprendizado de máquina conforme já destacado no subcapítulo 3.2 é uma subcategoria de uma Inteligência Artificial ainda completamente inatingível verdadeiramente e auto-sustentável, que incluindo a segurança cibernética. A *machine learning* se mostra como um mecanismo de verificação aprimorado, que aumenta a velocidade de detecção e maior capacidade de detectar irregularidades no IA. Isso contribuiu para um maior nível de proteção dos sistemas de IA, especialmente no que tange as ameaças novas e emergentes bem como ameaças persistentes avançadas (*advanced persistent threats* - APTs).

[13] MUNHOZ, Vinicius. WannaCry, o ransomware que fez o mundo chorar na sexta-feira (12). *In*: TECMUNDO. [S.I.], 12 de maio de 2017. Disponível em:

No segundo momento, a operação então denominada de *Doublepulsar,* atacou as vulnerabilidades *backdoors* e implantou, nos equipamentos dos usuários-alvo, os códigos maliciosos e totalmente camuflados. Ao contrário do *WannaCry* de objetivo monetário, o *Doublepulsar* objetiva angariar informações importantes para dominar o sistema de informática do usuário. Com sua característica de camuflagem, torna-se impossível desvendar sua aparência no sistema.[14]

Apesar de a inteligência artificial guardar o dever de observância com atuação célere do *malware* por motivos de segurança do próprio sistema a ser estruturado, a IA, de modo versátil, também pode ser mostrar eficiente na prevenção do próprio malware, uma vez que, atualmente, a batalha contra *malware* sempre foi reativa frente aos cibercriminosos, necessitando de proatividade.

Em outras palavras, um ataque cibernético se lança na rede, acaba infectando os sistemas proliferados no mundo afora e, concomitantemente, as empresas de antivírus iniciam uma jornada para buscar proteções aos seus clientes. Contudo, ainda que empresas *experts* tentem domar o *malware* previamente por meio de emissão de atualizações aos seus clientes, destaca-se que essa não se mostra uma alternativa adequada, pois demanda o tempo dos bons para perseguir os cibercrimosos, que, muitas vezes, já realizaram estrados imensuráveis.

Como não há meios de avançar-se no tempo, de modo a obter-se o conhecimento prévio dos acontecimentos destrutivos do *malware*, uma vez que a humanidade caminha tão-somente com diferença de fusos horários, há concordância que todos partimos do mesmo ponto de partida para os ataques de malware serem identificados. É nesse sentido que exsurge a inteligência artificial para antever possíveis ataques nas redes de computadores.

---

https://www.tecmundo.com.br/malware/116652-wannacry-ransomware-o-mundo-chorar-sexta-feira-12.htm. Acesso em: 30 jun. 2020.

[14] PERLROTH, Nicole. A Cyberattack ‘the World Isn’t Ready For’. In: THE NEW YORK TIMES. Nova York, 22 de junho de 2017. Disponível em: https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html. Acesso em: 20 jul. 2018.

A inteligência artificial e a subárea *machine learning* vêm sendo utilizadas para diariamente colher dados de nossas vidas. Larry Page, em setembro de 1998, teve esse *insight* quando lançou o pesquisador Google, que se retroalimentou das nossas pesquisas. Em outras palavras, se acordamos no domingo e acreditarmos que estamos livre de assédios das empresas de colheita de dados, é um ledo engano, pois até a pesquisa pela picanha ou entrecot bovino para o churrasco por meio do *smartphone* já demonstra nossa preferência pelos cortes de carnes. Assim, na segunda, quando abrirmos o primeiro site, na barra lateral, estará lá o oferecimento do nosso almoço de domingo para o almoço ou para a janta de segunda.

A Amazon identifica os metadados de buscas dos usuários da rede para identificar suas preferências de compra. O Mercado Livre guarda todos os dados de pesquisas e monta um perfil de consumo de cada usuário, que oferece um *rol* de produtos indicados ao usuário quando a *homepage* é aberta. Esses poucos exemplos, todos presentes no nosso cotidiano da vida moderna, acabam criando razões suficientes para utilizarmos a inteligência artificial como ferramenta de prevenção a ataques de malware, uma vez que há uma magnitude de dados que necessitam da inteligência artificial para poder ser bem trabalhados, que precisam ser processados com alta velocidade.

A inteligência artificial abarca as condições propícias de manipulação de dados de maneira inigualáveis. Por isso, a inteligência artificial, por meio de suas subáreas *machine learning* e *deeep learning,* assume papel importante no combate aos cibercriminosos, uma vez que a equipe de *data science* trabalha, em regra, com o *data set* algo em torno de 80% do tempo para finalização do projeto. É sempre importante ressalvar que a manipulação dos dados é fundamental para o sucesso do combate e identificação das fraudes.

Os bancos e operadoras de cartão de crédito foram os primeiros a utilizarem o aprendizado de máquina. Como os bancos e operadoras de cartão de crédito possuem um *data set* muito bem trabalhado dos seus clientes, uma vez que, para a concessão de crédito, os bancos exigem uma enormidade de dados e comprovações dos seus clientes, a inteligência artificial exsurge para identificar as transações que podem ser fraudulentas. Isso ocorre quando o sistema de IA identifica, com base no *data set* construído para aquele cliente, dados inconsistentes – a exemplo, o local de IP da máquina diferentemente do

usualmente utilizado para a compra. A partir disso, um dispositivo como um telefonema para o cliente é acionado para certificação. Isso deriva do uso da inteligência artificial, oriundo do aprendizado de máquina constituído que identifica a eventual transição suspeita de fraude.

A referida ferramenta de análise de comportamento de usuários é comumente utilizada para buscar soluções de segurança, usando algoritmos de aprendizados de máquina, construídos a partir de dados muito bem trabalhados, que monitoram na verdade todos os passos do usuário. Isto é, o aprendizado de máquina determina, a partir do *data set*, um comportamento esperado, ou dito como normal do usuário, utilizado para identificar desvios ou anomalias, que potencialmente abririam a porta para os cibercriminosos plantarem um *walmare*.

Nota-se, que o avanço do *software* malicioso representa um enorme desafio de proteção de redes e de sistemas de computadores contra os ataques maliciosos, posto a sofisticação da conduta dos cibercriminoso. Assim como a IA, o *malware* também está em constante evolução e obriga os analistas de segurança e pesquisadores a manterem um acompanhamento constante, melhorando suas defesas cibernéticas. O aumentou de *malware* se dá em função do uso de polimórficos, de modo a modificar o mecanismo polimórfico para realizar uma mutação no código e manter sua funcionalidade original; já as técnicas metamórficas usadas para escapar da detecção e esconder seu rastro, reescrevem seu código para um equivalente sempre que propagado.

Os cibercriminosos de *malware* podem usar várias transformações técnicas, mas não se limitando à renomeação de registro, à permutação de código, à expansão de código, à redução de código e à inserção de código de lixo. A combinação das técnicas acima mencionadas resultou rapidamente no volume crescente de *malware*, fazendo as investigações forenses de *malware* em casos demorados, caros e mais difíceis.[15]

Nesse sentido, os analistas de segurança estão sempre melhorando suas defesas, de modo a acompanhar os possíveis ataques dos malwares, que se

[15] GIBERT LLAURADÓ, Daniel; MATEU PIÑOL, Carles; PLANES CID, Jordi. The rise of machine learning for detection and classification of malware: Research developments, trends and challenge. **Journal of Network and Computer Applications**, v. 153, p. 1-22, jan. 2020. Disponível em: https://repositori.udl.cat/bitstream/handle/10459.1/68344/030101.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2020.

entendem como pré-estabelecidos; somente não se sabe ao certo o *modus operandi* do novo *malware* a exsurgir. Por isso, tecnicamente, tem-se como essencial a proteção de ponto final,[16] que fornece um conjunto de programas de segurança, incluindo, ainda, *firewall*, filtragem de *URL*, e-mail de proteção, anti-spam e *sandboxing*. Especificamente, *software* anti-malware fornece a última camada de defesa.

Com a evolução do *malware*, as soluções AV se tornaram responsáveis pela prevenção, detecção e remoção de *software* malicioso instalado no dispositivo de ponto final. Contudo, as soluções AV são baseadas em assinaturas e nos métodos baseados em heurística. Ocorre que, enquanto a assinatura é um algoritmo ou *hash* que identifica exclusivamente um *malware* específico, as heurísticas são um conjunto de regras determinado por especialistas somente após analisar o comportamento do *malware* já identificado.

Assim, nota-se que, nas abordagens referenciadas, há uma exigência prévia que o *malware* seja analisado, antes da definição das regras e heurísticas, o que não sugere uma prevenção contra-ataques de *malwares*, mas uma proatividade diante o ataque do cibercriminoso.

No tocante, o estudo de Ajit Kumar e*t al*. (2017) demonstrou e evidenciou que *malware* é um dos principais obstáculos para a expansão e o crescimento da aceitação do avanço tecnológico. Enfatizou-se nesta pesquisa que tanto as empresas quanto os usuários comuns estão lutando para se proteger contra o *malware* no ciberespaço. Por isso, sabe-se da importância do desenvolvimento de métodos eficientes de detecção de *malware*.[17] O estudo também ofereceu

---

[16] Uma das grandes vantagens da proteção *endpoint* é a possibilidade de atuar analiticamente, verificando arquivos com maior cuidado e precisão na hora de estabelecer quais são ameaças e quais não. Além disso, a garante uma defesa mais abrangente do que os antivírus. Isso porque, em alguns casos, pode ser acionada em conjunto uma ferramenta de análise e utilizar informações de bancos de dados de fornecedores. O *endpoint* entrega proteção mais proativa, indo além da prevenção de ataques de malwares. Isso ocorre porque, graças aos recursos de criptografia e proteção de dados, ele atua evitando perda de informações e no monitoramento de equipamentos. XIAO, Claud; CHEN, Jin. New OS X Ransomware KeRanger Infected Transmission BitTorrent Client Installer. *In*: PALO ALTO NETWORKS BLOG. Santa Clara, Califórnia, EUA: 06 de março de 2016. Disponível em: http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-kerangerinfected-transmission-bittorrent-client-installer/. Acesso em: 20 jul. 2020.

[17] KUMAR, Ajit; KUPPUSAMY, K. S.; GNANASEKARAN, Aghila. A learning model to detect maliciousness of portable executable using integrated feature set. **Journal of King Saud University**, India, v. 31, n. 2, jan. 2017. Disponível em: http:// dx.doi.org/10.1016/j.jksuci.2017.01.003. Acesso em: 12 fev. 2020.

uma solução baseada em aprendizado de máquina para classificar uma amostra como benigna ou malware com alto precisão e baixo *overhead* de computação.

Foi estruturado um conjunto de recursos integrados e amalgamado como uma combinação de campos de cabeçalho executáveis portáteis, valor bruto e valores derivados. Vários algoritmos de aprendizado de máquina como árvore de decisão, floresta aleatória, kNN, regressão logística, análise discriminante linear e Naive Bayes foram adotados na classificação de malware. Usando o conjunto de recursos brutos existente e o proposto conjunto de recursos integrados, os autores verificaram o desempenho de cada classificador. Desse modo, a evidência empírica indicou 98,4% de precisão de classificação na validação cruzada de 10 vezes para o conjunto de recursos integrado proposto. Num novo conjunto de dados de teste, a precisão foi observada como 89,23% para o sistema integrado conjunto de recursos que representa uma melhoria de 15% na precisão alcançada com o conjunto de recursos brutos sozinho.

A diferença de um arquivo executável portátil (PE) malicioso para um benigno é muito importante, pois o formato de arquivo PE é o formato de arquivo muito usado, usado no sistema operacional Windows. A pesquisa de Ajit Kumar *et al.* (2017) forneceu uma nova engenharia de recursos técnicos que melhorou o desempenho do aprendizado de máquina classificador baseado em detecção de arquivo PE malicioso.

A técnica proposta usou a análise estática para extrair os recursos que, por se tratar da abordagem estática, necessita menos tempo e recursos do que a análise dinâmica. Assim, foi comparado o desempenho do recurso integrado proposto com o recurso bruto definido pelo treinamento e pelo teste de diferentes classes de algoritmos de aprendizado de máquina. Isso acabou destacando o bom desempenho de classificadores, que melhorou significativamente com o novo integrado conjunto de características.

Para registrar um desempenho robusto e estável de classificadores, a validação foi realizada com quatro diferentes métodos: divisão de treinamento e teste, validação cruzada de 10 vezes, novo teste conjunto de dados e a*rea under curve* (AUC) parcial. Com todos os quatro métodos reunidos, o recurso integrado conjunto foi executado com maior eficácia do que o conjunto de recursos brutos.

Outro estudo publicado, no ano de 2019, por pesquisadores da Universidade de Lleida na Espanha, apresentou um método prévio de identificação de *malwares* por meio do aprendizado de máquinas. O objetivo do *malware analysis* é fornecer informações sobre as características, finalidade e comportamento de um determinado *software*, dividido em análise estática e dinâmica.[18]

A análise estática busca examinar um executável sem autorização para execução[19], ao passo que a análise dinâmica observa o comportamento do executável quando buscar realizar a execução sem autorização do usuário.[20]

Destaca-se que ambos os tipos têm suas vantagens e limitações. A estática se mostra mais ágil; porém, se o *malware* for ocultado por códigos, pode ocorrer de sua detecção ficar ofuscada. De outra banda, os códigos ofuscados e os *malwares* polimórficos dificilmente fogem da análise dinâmica no decorrer da execução do programa; nota-se uma espécie de complementação.

Contudo, com o ritmo de novos ataques e variantes, a detecção de *malware* tradicional e da análise de *malware* não são acompanhadas pela análise dinâmica. Tampouco com a estática, a complementariedade das análises

---

[18] GIBERT LLAURADÓ, Daniel; MATEU PIÑOL, Carles; PLANES CID, Jordi. The rise of machine learning for detection and classification of malware: Research developments, trends and challenge. **Journal of Network and Computer Applications**, v. 153, p. 1-22, jan. 2020. Disponível em: https://repositori.udl.cat/bitstream/handle/10459.1/68344/030101.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2020.

[19] A análise estática consiste em examinar o código ou estrutura do arquivo executável sem executá-lo. Este tipo de análise pode confirmar se um arquivo é malicioso, forneça informações sobre sua funcionalidade e pode ser usado para produzir um conjunto simples de assinaturas. Por exemplo, o método mais comum usado para identificar exclusivamente um programa malicioso é *hash*. GIBERT LLAURADÓ, Daniel; MATEU PIÑOL, Carles; PLANES CID, Jordi. The rise of machine learning for detection and classification of malware: Research developments, trends and challenge. **Journal of Network and Computer Applications**, v. 153, p. 1-22, jan. 2020. Disponível em: https://repositori.udl.cat/bitstream/handle/10459.1/68344/030101.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2020. p. 4.

[20] A análise dinâmica envolve a execução do programa e o monitoramento do seu comportamento no sistema. Isso normalmente é realizado quando a análise estática chegou a um beco sem saída, seja devido à ofuscação ou por ter esgotou as técnicas de análise estática disponíveis. Ao contrário da análise estática, ele rastreia as ações reais executadas pelo programa. No entanto, a análise deve ser executada em um ambiente seguro para não expor o sistema a riscos desnecessários, onde o sistema é a máquina executando a ferramenta de análise e o resto das máquinas da rede. Para este fim, máquinas físicas ou virtuais dedicadas são configuradas. As máquinas físicas devem ser configuradas em redes sem ar, isto é, redes isoladas onde as máquinas estão desconectadas da Internet ou qualquer outra rede, para evitar a propagação de malware. O principal A desvantagem das máquinas físicas é este cenário sem conexão com a Internet, pois muitos programas maliciosos dependem da conexão com a Internet para atualizações, comando e controle e outros recursos (Ibid., p. 4).

não consegue acompanhar a dedicação dos cibercriminosos com *malware* cada vez mais diversificado. São milhares de ataques que os usuários devem se preocupar rotineiramente, além de enfrentarem uma escassez de profissionais que atuam da segurança cibernética[21]. Costuma-se dizer que não é como ir ao mercado buscar um profissional das profissões tradicionais.[22]

Eis que, nesse cenário, o aprendizado de máquina é o meio para modificar essa corrida, de modo a tentar igualar o poder de armas, uma vez que a capacidade de manter um *dataset* com uma farta gama de dados para fazer frente aos ataques dos cibercriminosas é uma característica no *machine learning*. Os *experts* da segurança cibernética asseguram que a inteligência artificial exsurgiu em boa hora, pois, além de dinamizar diversas áreas do conhecimento, também venho para auxiliar a área da cibersegurança. A IA possui condições de possibilidade de prevenção, uma característica notável que realmente pode evitar ataques, e não somente barrá-los após seus perspicazes danos.[23]

Possivelmente, esse aumento das pesquisas advém além do próprio avanço da computação que incrementou significativamente a área de atuação do *malware*. Na última década também houve um aumento na pesquisa e na implantação de soluções de aprendizado de máquina para lidar com as tarefas de detecção e de classificação de *malware*. O sucesso e a consolidação de abordagens de aprendizado de máquina não teriam sido possíveis sem a confluência de três desenvolvimentos recentes: (i) aumento de *feeds* rotulados de *malware,* o que significa que, pela primeira vez, *malware* rotulado está disponível não apenas para a comunidade de segurança, mas também para a comunidade de pesquisa; (ii) a pujança do poder computacional aumentado rapidamente e também com custo acessível a maioria dos pesquisadores; e (iii)

---

[21] Yuval Noah Harari em sua obra Homo Deus – Uma breve história do amanhã discorre que: “Embora alguns especialistas conheçam bem os desenvolvimentos em algum campo, como é o caso da inteligência artificial, da nanotecnologia, de megadados ou da genética, ninguém é especialista em tudo. Ninguém, portanto, é capaz de ligar todos os pontos e enxergar o quadro completo. HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. Tradução de Paulo Geiger. 1. ed. São Paulo: Companhia das Letras, 2016. p.59.

[22] HARARI, Yuval Noah. **Sapiens**: Uma breve história da humanidade. Tradução de Janaína Marcoantonio. 38 ed. São Paulo: L&PM Editores, 2018. p. 408-426.

[23] Isso é corroborado com a pesquisa de trabalhos no Google Scholar, que no ano de 2020 aponta 2.340 pesquisas abordando a IA - *machine learning* auxiliando a cibersegurança, um aumento de 30% em relação a 2019, e comparado a 2010, representa um incremento exponencial de 550%.

a evolução da *machine learning* em um ritmo cada vez maior durante as últimas décadas, com ampla gama de tarefas, como computador visão, reconhecimento de fala e processamento de linguagem natural.[24]

No tocante, com o auxílio do *machine learning,* a abordagem abarcou três possibilidades: o estático, o dinâmico e o híbrido. O estático, por suposto, extrai recursos da análise estática do *malware*; já a abordagem dinâmica se ocupa com a análise dinâmica, enquanto uma terceira abordagem, a híbrida, utiliza ambas as abordagens, tanto o estático quanto o dinâmico. Contudo, a cibersegurança também se apropria das redes neurais artificiais, que vem mostrando um bom desempenho no *malware* domínio.[25]

O trabalho de pesquisa de Gibert. *et al*. (2019)[26] exsurgiu em virtude do avanço das ferramentas da IA para detecção de *malware* referenciado anteriormente, com o objetivo de explorar as abordagens estáticas, dinâmicas e híbridas tidas como tradicionais. Isso, no modo de ver dos autores, mostram-se incompletas dado o avanço de *malware*. A pesquisa destinou-se a apoiar os analistas de segurança para que pudessem aplicar o aprendizado de máquina nos três métodos referenciados, de modo a automatizar parte do processo de

---

[24] O tamanho desses feeds varia de amostras limitadas de alta qualidade, como os fornecidos pela Microsoft (RONEN, Royi *et al*. Microsoft Malware Classification Challenge. **ArXiv**, p. 1-7, fev. 2018. Disponível em: https://www.researchgate.net/publication/323470001_Microsoft_Malware_Classification_Challenge?channel=doi&linkId=5a975f580f7e9ba42974d01b&showFulltext=true. Acesso em: 20 jan. 2020) para o Big Inovadores de dados reunindo desafio de previsão de antimalware para grandes volumes de malware, como theZoo (THE ZOO. In: GITHUB. [S.I.]: Yuval Nativ, L.L., 2015. Disponível em: https://github.com/ytisf/theZoo. Acesso em: 20 jan. 2020) ou VirusShare (VIRUS SHARE. In: VXSHARE. [S.I.], 2011. Disponível em: https://virusshare.com/. Acesso em: 20 jan. 2011). GIBERT LLAURADÓ, Daniel; MATEU PIÑOL, Carles; PLANES CID, Jordi. The rise of machine learning for detection and classification of malware: Research developments, trends and challenge. **Journal of Network and Computer Applications**, v. 153, p. 1-22, jan. 2020. Disponível em: https://repositori.udl.cat/bitstream/handle/10459.1/68344/030101.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2020.

[25] Para exemplificar, estudos recentes demonstram a construção de uma rede neural convolucional para determinar o grau de impacto de executáveis do PE a partir dos bytes brutos do próprio arquivo. A motivação por trás das abordagens de redes neurais é criar detecção sistemas que não confiam no conhecimento dos especialistas no domínio para definir características discriminativas. RAFF, Edward *et al*. An investigation of byte n-gram features for malware classification. **Journal of Computer Virology and Hacking Techniques**, v. 14, n. 1, p. 1-20, 2018. Disponível em: https://doi.org/10.1007/s11416-_016-_0283-_1. Acesso em: 12 jan. 2020

[26] GIBERT LLAURADÓ, Daniel; MATEU PIÑOL, Carles; PLANES CID, Jordi. The rise of machine learning for detection and classification of malware: Research developments, trends and challenge. **Journal of Network and Computer Applications**, v. 153, p. 1-22, jan. 2020. Disponível em: https://repositori.udl.cat/bitstream/handle/10459.1/68344/030101.pdf?sequence=1&isAllowed=y. Acesso em: 20 mar. 2020.

análise de *malware* e, assim, possibilitar uma compreensão geral dos métodos atualmente em uso, bem como das suas novas tendências.

O estudo ainda forneceu uma descrição de métodos neurais com o objetivo de detectar e de classificar o *malware*,[27] uma vez que, segundo o estudo, as redes neurais superam os recursos de aprendizagem de dados brutos em vários campos. Verdadeiramente, o avanço da IA impulsionou o aprendizado de máquinas, que replicou no incremento das redes neurais no *malware* domínio.[28]

Ambas as pesquisas demonstraram que a IA, por meio da *machine learning* e das redes neurais, vem oferecendo uma resposta à altura dos ataques de *malware*, que acabou nivelando as forças entre a cibersegurança e os cibercriminosos. Isso ocorre seja com a *machine learning* se utilizando das três abordagens, que são o estático, o dinâmico e o híbrido, seja pelas redes neurais que manipulam com maior performance os dados brutos, fazendo frente ao combate de malware.

Contudo, todo e qualquer projeto de sistema de IA deve, indiscutivelmente, buscar bloquear as possibilidades de ataques de *malware*. Isso porque, quanto maior e mais notório o sistema de IA for, o ataque dos cibercriminosos também será mais sofisticado para burlar a segurança do sistema de IA. Essa é outra especificidade que deve estar presente diante do avanço tecnológico. Ainda, sem deixar de considerar o futuro potencial da computação quântica que terá capacidade de processamento capaz de quebrar a mais segura criptografia[29]; essas são outras especificidades que o Poder

---

[27] Os *malwares* foram categorizados de acordo com a forma como a entrada é pré-processada antes da alimentação rede neural, bem como uma breve descrição da aprendizagem multimodal abordagens (Ibid., p. 4).

[28] Por exemplo, os autores (RAFF et al, 2018) propôs a construção de uma rede neural convolucional para determinar a maldade dos executáveis PE a partir dos bytes brutos do próprio arquivo. A motivação por trás das abordagens de rede neural é construir detecção sistemas que não dependem do conhecimento dos especialistas do domínio para definir características discriminativas (RAFF et al, 2018, p. 2).

[29] A questão sempre foi exatamente quando esse dia chegaria. A técnica de criptografia digital mais comum, RSA, que foi inventada em 1977, é baseada na multiplicação de dois grandes números primos. Uma maneira de quebrá-lo é descobrir o que eram aqueles dois grandes primos. Em 1994, o matemático Peter Shor inventou um algoritmo que, se executado em um computador quântico suficientemente poderoso, encontraria facilmente esses dois primos. Mas, na época, os computadores quânticos ainda eram máquinas puramente teóricas. Contudo, no ano passado, o Google afirmou ter alcançado um marco conhecido como “supremacia quântica”, tendo construído um computador quântico capaz de realizar um cálculo que não poderia ser feito em um computador tradicional em um período razoável. Em 2016, a Agência de Segurança Nacional dos Estados Unidos emitiu um alerta severo de que as agências governamentais e as empresas “devem agir agora” para começar a migrar para um novo padrão de criptografia que esteja protegido contra ataques quânticos baseados em

Judiciário deve ter presente diante do avanço tecnológico, pois caso contrário, permanecerá experimentando os ataques de *malware* rotineiramente.

Enfim, após visitar a complexa área da Ciência da Computação, de modo a entender os limites de aplicabilidade dos sistemas de IA no Direito, e como dito, no início deste capítulo, primeiro compreender para depois sim, falar do objeto. Em especial, nessa quadra da história, salientar os limites de aplicabilidade dos sistemas de IA no Direito, em face da presença indiscutível dos vieses algoritmos e ausência da *accoutability.* Assim, com essa pequena bagagem de conhecimento da Ciência da Computação, apresentar-se-á no próximo e último capítulo, a resposta à pergunta desta tese: se a inserção do sistema de IA Victor, no processamento das questões de repercussão geral de matérias tributáias submetidas ao STF, dimuiria o número de processos tributários sobrestados no país?

computador. Porém, ninguém sabe ao certo qual deverá ser o padrão de criptografia. Esses novos métodos de criptografia "pós-quântica" e de assinatura digital provavelmente se tornarão obrigatórios para todos os departamentos do governo dos Estados Unidos e para muitas empresas que fazem negócios com o governo, especialmente em defesa e inteligência. KAHN, Jeremy. Quantum computers threaten to end digital security. Here's what's being done about it. In: FORTUNE. [S.l.], 11 de setembro de 2020. Disponível em: https://fortune.com/2020/09/11/post-quantum-encryption-algorithm-nist/amp/?__twitter_impression=true. Acesso em: 21 nov. 2020.