Antivírus

Marcelo Feliz nº50356

Abstract

No presente artigo será abordado, de forma sucinta, o tema software de antivírus, o seu funcionamento, evolução ao longo do tempo, bem como o que podemos esperar no futuro. Serão também descritas diversas técnicas de deteção de vírus e/ou malware. Com o crescimento exponencial dos vírus e de malwares, os softwares de antivírus e as suas técnicas de deteção e eliminação das ameaças, tornam-se cada vez mais importantes no dia-a-dia dos utilizadores. A evolução dos vírus e dos diversos tipos de ameaças levou, consequentemente, à constante atualização e aperfeiçoamento dos antivírus, de forma a fazer face a todas as ameaças existentes. O futuro na área do software de antivírus passa pelo aprofundamento do estudo e dos métodos e de todos os tipos de inteligência artificial, utilizadas a favor dos antivírus.

Keywords— software de antivírus, malware, vírus, inteligência artificial

1 Introdução

Os antivírus são programas que usam um sistema operativo, e que têm como função prevenir, detetar e eliminar vírus e malware do dispositivo. Originalmente foi desenvolvido este tipo de software de antivírus para detetar e remover vírus de computador. No entanto, com o surgimento e aumento de outros tipos de malware, este tipo de software começou a proteger o computador de outros problemas. O Malware é um software construído de modo a causar algum dano no sistema de informação. Os mesmos constituem-se como ameaças que estão em constante evolução e podem causar diversos danos no dispositivo. [4] O uso de antivírus objetiva o aumento da proteção do dispositivo, sendo utilizado, maioritariamente, com um caráter preventivo. O mesmo utiliza diversas técnicas e métodos para detetar o malware. [4]

Na atualidade muitos antivírus tentam defender os utilizadores, de diversas ameaças, para além de vírus, como por exemplo, (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraud tools, adware, and spyware. Há ainda antivírus que com as suas versões premium incluem proteções adicionais tais como infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT), and botnet DDoS attacks. [4]

Existem diversas formas de um dispositivo contrair um vírus. Os mesmos podem aparecer por meio de pendrives, emails, sites de conteúdo duvidoso, download de arquivos e programas infetados e por vários outros meios. Esses vírus e códigos maliciosos possuem a finalidade de interferirem no funcionamento do computador ou outro aparelho para registar, corromper, destruir dados e transferir informações para outros dispositivos.
[11]

Desde o surgimento do primeiro vírus, as ameaças informáticas têm crescido exponencialmente, sendo utilizadas por mais utilizadores, de forma mais perigosa. Existem diversas organizações que procuram combater a disseminação do malware. Saliento, o Computer Antivirus Research Organization (CARO) e o European Institute for Computer Anti-Virus Research (EICAR). O CARO foi fundado em 1990, com o objetivo de aprofundar o estudo e a compreensão sobre o malware. O EICAR foi fundado pelos membros do CARO, em 1990, com o objetivo de disseminar a informação sobre os vírus e o malware, estando neste momento com diversos projetos ativos. [7]

O restante deste artigo está estruturado da seguinte forma. Na secção 2, será referido um pouco da história do surgimento do software de antivírus. Na secção 3, será especificado o funcionamento dos antivírus, bem como alguns dos tipos de antivírus, de acordo com o seu objetivo e finalidade, e por último, será abordada questão do futuro do software de antivírus. Por último, na secção 4, serão identificadas algumas das desvantagens da utilização dos antivírus.

2 História

O surgimento de antivírus deu-se na década de 80. Inicialmente, os antivírus eram denominados de scanners, os mesmos eram desenvolvidos como linhas de comando, que procuravam identificar padrões duvidosos, em diversos programas. Os primeiros antivírus eram produtos unidimensionais, que dependiam de assinaturas para identificar vírus. Contudo, este tipo de antivírus não conseguia detetar novas ameaças, sendo que devido ao grande crescimento de vírus informáticos, este tipo de antivírus deixou de ser viável. O primeiro antivírus a ser criado foi o McAfee, por John McAfee, em 1987, denominado de Virusscan. [9]

Devido ao crescimento exponencial de ameaças informáticas a que os utilizadores estão sujeitos todos os dias, os antivírus têm evoluído de forma considerável. Na década de 90, era comum que uma empresa de antivírus recebesse alguns programas duvidosos, no espaço de uma semana, hoje em dia, uma empresa de antivírus recebe milhares de ficheiros duvidosos todos os dias. Este crescimento exponencial de ameaças informáticas levou a que as empresas de antivírus apostassem na deteção automática e na criação de heurísticas, para a deteção de vírus informáticos. A existência de vírus informáticos, de diferentes tipos e particularidades forçou a industria dos antivírus a crescer exponencialmente, nos últimos 15 anos. [4] [8]

Por sua vez, também os vírus informáticos evoluíram drasticamente. O primeiro vírus informático foi criado em 1971, pelo BBN technologies, tendo-lhe sido atribuído o nome de Crepper. O mesmo era um vírus que se auto-replicava e que atacava o disco rígido do dispositivo, até que o mesmo parasse de funcionar. Desde então, têm surgido diversos vírus e ameaças. Inicialmente, os motivos que levavam ao desenvolvimento de vírus informáticos eram o reconhecimento e o sentido de desafio que os indivíduos sentiam. Contudo, hoje em dia, o principal motivo para o desenvolvimento de vírus é o dinheiro. O desenvolvimento de vírus informáticos é uma indústria altamente rentável, utilizada para extorquir dinheiro dos utilizadores, bem como as suas credenciais de vários serviços online. [4] [8]

Tendo e conta que os primeiros vírus informáticos eram mais simples, também a sua deteção por programas de antivírus era um processo relativamente simples. Atualmente, a deteção de vírus informáticos é muito mais complexa. O crescimento dos vírus informáticos, da sua complexidade e diversidade, levou ao desenvolvimento de programas de antivírus mais eficientes, nomeadamente os denominados next-generation antivírus. Enquanto que os antivírus tradicionais conseguiam proteger contra ameaças já conhecidas e dependiam de recursos humanos, os next-generation antivírus protegem contra novas formas de ameaças e utilizam uma análise preditiva realizada através do dispositivo e da inteligência artificial, de forma a conseguirem identificar e proteger os dispositivos contra o vírus. Atualmente, os antivírus conseguem proteger os dispositivos de inúmeras ameaças, como Browser Helper Objects, browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses (cavalo de tróia), worms, entre outras. [5]

3 Funcionamento

Os antivírus ajudam a proteger o sistema e a informação. No entanto, mesmo que tenhamos antivírus instalados e saibamos que o mesmo se encontra sempre a correr em segundo plano, é crucial compreender como funciona um antivírus. Se soubermos um pouco melhor como o antivírus funciona então estaremos melhor equipados para nos protegermos, mantendo os programas atualizados e mais eficientes na proteção de vírus e outras ameaças. [3] [4]

Os vírus deixam "pegadas" virtuais por usarem as suas assinaturas únicas quando se movem de um sistema para outro. Pelo facto de o vírus usar a mesma assinatura em todo o lado, o software pode guardar a assinatura para descobrir se esse vírus entrou no nosso sistema. O que faz um vírus difícil de encontrar são as variações que as pessoas criam para modificar vírus já existentes. Por exemplo, o mesmo vírus pode ter muitos nomes diferentes, isto porque as pessoas podem usar código de vírus que já existem e alterar as suas especificações, alterando a assinatura, tornando o vírus irreconhecível. Contudo, ainda que a assinatura seja diferente, irá ser semelhante à original porque a maior parte do código vai ser igual à original. ´ [3] [4]

Através das assinatura dos vírus, os antivírus defendem-se de malware. O software de defesa usa uma base de dados de assinaturas de vírus conhecidos e procura no sistema por essas assinaturas. Por exemplo, se o utilizador decidir clicar num link que não esteja totalmente familiarizado. Este link pode ser um vírus disfarçado de outra coisa, como por exemplo um programa útil. O que o antivírus vai fazer é, confirmar na base de dados e perceber se a assinatura é conhecida de algum vírus. No caso de alguma variação ter sido feita no vírus, esta pode ser suficiente para ludibriar o sistema de defesa e não ser detetado pelo software. [3] [4]

Novos vírus são criados muito rapidamente, sendo por isso que devemos tentar ter sempre o dispositivo atualizado, porque deste modo, também a base de dados do antivírus estará atualizada. Isto significa que temos de adicionar todas estas novas assinaturas de vírus novos na base de dados do sistema. Se esta não estiver atualizada o antivírus não saberá identificar novos vírus como possíveis ameaças. [3] [4]
Existem inúmeras formas e técnicas de um antivírus detetar e eliminar o malware e os vírus, pelo que algumas delas são: imunizadores, residentes, baseadas em assinaturas (ou scanning), baseadas em heurísticas, baseadas no comportamento, emulação de código e técnicas de mineração de dados.

As técnicas baseadas em heurísticas são utilizadas, normalmente, em simultâneo com as técnicas baseadas em assinaturas, detetando o vírus através das suas características já conhecidas. Esta deteção baseada em heurísticas consegue detetar o malware através da análise estatística dos ficheiros, à procura de características suspeitas, sem uma assinatura exata. Por exemplo, o antivírus pode analisar a presença de instruções duvidosas ou de código indesejável. A análise heurística divide-se em duas categorias: heurística estática e heurística dinâmica.

Heurística estática diz respeito a várias técnicas de heurística que tentam verificar a presença ou não de malware num programa suspeito, examinando a estrutura e o conteúdo do programa através de um estado inativo e procurando encontrar fragmentos de código que são frequentemente utilizados para malware. A grande vantagem da utilização da Heurística estática é que ao contrário da utilização da Heurística dinâmica, a mesma consegue analisar vários caminhos possíveis de execução do programa, pois a mesma olha para todo o conteúdo do programa, enquanto que a heurística dinâmica analisa apenas a parte do código utilizada durante uma invocação específica do programa.

As Técnicas baseadas no comportamento funcionam de forma semelhante aos antivírus baseados em heurísticas, mas em vez de analisarem o código, analisam as ações do dispositivo, conseguindo detetar o malware depois da sua ação. A técnica de emulação de código é uma das técnicas mais fortes na deteção de malware, estimula o processador central do computador, a memória, o armazenamento e ainda algumas funções do sistema operativo, de forma a correr o malware virtualmente e analisar o seu comportamento. Assim, o malware não age no próprio dispositivo, sendo controlado pelo dispositivo virtual. Por último, as técnicas de mineração de dados, são uma das técnicas mais recentes de deteção de vírus e malware. As mesmas conseguem identificar e classificar o comportamento de um determinado ficheiro, a partir de uma série de características do ficheiro. [4] [2] [5] [10] [**upadhyay**]

Um antivírus é um sistema complexo que pode utilizar diversos métodos e técnicas para a deteção de vírus e malware. A figura 1 mostra o funcionamento de um software de antivírus típico. Como podemos ver, o mesmo utiliza diversas técnicas, para detetar o vírus e/ou malware, nomeadamente, assinaturas, heurísticas, comportamento e emulação de código. [2] [6] [**aryanbypassing**] [**upadhyay**]

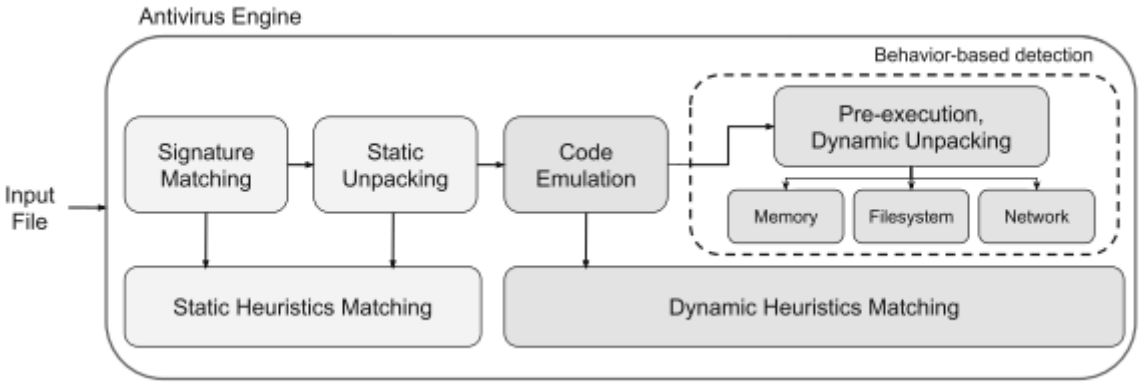

Figure 1: Funcionamento tipico de um AntiVírus

Um software de antivírus necessita de possuir diversas características básicas e fundamentais, nomeadamente, o mesmo necessita de conseguir verificar ficheiros compactados, um driver de auto-proteção para se proteger contra o ataque do malware, funcionalidade de firewall e inspeção de rede, linhas de comando e ferramentas de interface gráfica, devem possuir um scanner, de forma a conseguir analisar o sistema, quando o utilizar o solicitar, deve possuir diversas assinaturas, de modo a conseguir determinar se um ficheiro é duvidoso. [4]

3.1 Tipos de Antivírus

Com a evolução dos antivírus, foram surgindo diversos tipos de antivírus, que variam de acordo com a sua finalidade e o seu objetivo. Neste sentido, no que diz respeito à finalidade, os antivírus podem ser classificados em preventivos, identificadores e descontaminadores. Os antivírus preventivos antecipam a entrada de um malware no dispositivo. Os mesmos analisam as ações e funções do sistema e avisam sobre uma possível ameaça. Os mesmos encontram-se, frequentemente, instalados na memória do dispositivo. Por sua vez, os antivírus identificadores, identificam as ameaças que poderão colocar em risco a eficiência do sistema. Os antivírus descontaminadores eliminam as ameaças que danificaram o dispositivo, procurando que o mesmo retorne ao seu desempenho inicial. [10] [4] [5]

Relativamente aos tipos de antivírus, de acordo com o seu objetivo, os mesmos podem ser classificados em Firewall, Antispyware, anti-pop-ups, antispam e antimalware. O firewall encontra-se dentro da categoria dos antivírus preventivos, pois o seu principal objetivo é o controlo da entrada e saída dos diversos programas. O Antispyware conseguem detetar e eliminar os spyware, que procuram acesso a informação pessoal do utilizador (e.g passwords). O anti-pop-ups identifica e previne todas as janelas pop-up que poderão surgir durante a navegação e poderão ocultar diversos spywares. O antispam previne o lixo eletrónico, ou seja, o spam. Por último, o antimalware, é caracterizado por ser um programa capaz de eliminar qualquer tipo de malware. [10] [4] [5]

3.2 O futuro dos Antivírus

Como tem sido referido, tem havido um crescimento exponencial de vírus e de ameaças, cada vez mais complexos e diversificados, pelo que também os softwares de antivírus têm de continuar em constante atualização e melhoria, de forma a fazer face a todas as ameaças. Posto isto, a inteligência artificial tem tido um papel crucial na evolução e aperfeiçoamento dos antivírus. Algumas das principais técnicas de inteligência artificial aplicada nos antivírus são a mineração de dados, as técnicas heurísticas e a rede neural artificial. A inteligência artificial é aplicada nos principais passos de deteção dos antivírus, ou seja, a deteção do vírus, análise do vírus e imunidade ao vírus. [1]

Relativamente ao método das heurísticas, esta é uma das técnicas mais populares com a utilização de inteligência artificial, sendo uma das técnicas com mais pesquisa científica. Esta técnica pressupõe que o antivírus tem o conhecimento e as ferramentas, de modo a usar métodos, que permitam verificar se existe ou não vírus, analisando, de forma inteligente, o código. Relativamente à técnica da mineração de dados, esta técnica pode ser utilizada para detetar dados, duvidosos e recentes de forma precisa e automática. Esta técnica deteta, automaticamente, padrões que se encontram na da base de dados, usando os mesmos para detetar algum malware.

Esta é uma técnica com bons resultados, sendo muito mais eficiente do que as técnicas tradicionais, como as assinaturas. No que diz respeito à técnica da rede neural artificial, a mesma surgiu como uma solução para a extração automática das assinaturas. Os métodos tradicionais para deteção de vírus e malware possuem algumas limitações, nomeadamente, os mesmos não conseguem extrair automaticamente todas as assinaturas, para além de questões de memória e capacidade. A técnica da rede neural artificial foi criada para fazer face a essas limitações, conseguindo detetar os vírus e malware em tempo real e em larga escala. [1]

As técnicas tradicionais utilizadas pelo software de antivírus, para detetar e eliminar o vírus e/ou malware, possuem diversas limitações, que dificultam a sua ação. O uso da inteligência artificial nos antivírus tem se revelado de extrema importância e eficácia, trazendo novos métodos, possibilitando a melhoria das técnicas de deteção de vírus e malware. O futuro na área do software de antivírus passa pelo aprofundamento do estudo e dos métodos, de todos os tipos de inteligência artificial, utilizadas a favor dos antivírus. [1]

4 Desvantagens na utilização de antivírus

Existem poucas desvantagens em usar software de antivírus, e as que existem são, normalmente, menos importantes do que os benefícios que as mesmas acarretam, tendo em conta o valor que proteger a informação do utilizador possa ter. [4]

Uma desvantagem da utilização de software de antivírus é a tendência de que muitos destes softwares vão abrandar o processamento do computador para o uso pessoal do utilizador. Isto porque o antivírus tem de verificar todos os ficheiros executáveis no sistema e compará-los com as assinaturas da base de dados. Este é um processo complexo e que ocorre em segundo plano e portanto pode ter como consequência abrandar o sistema. O trabalho do antivírus está a ser constantemente executado, mesmo que não se possa observar. Tudo o que se vai observar é que o sistema vai estar mais lento do que o normal. Felizmente, podemos combater esta desvantagem momentaneamente. Se precisarmos de executar software rapidamente podemos desativar momentaneamente o antivírus ou agendar um horário para o mesmo realizar esse processo. Um bom exemplo disto é desativar o antivírus para jogar jogos de computador e não deixar que este reduza a qualidade do jogo. [4]

Para além desta desvantagem, se o utilizador fizer uso de um antivírus gratuito, o mesmo não irá proteger o dispositivo contra todas as ameaças, pelo que é importante usar um firewall. Também as técnicas de deteção de vírus e malware são limitadas e as falhas de segurança podem ocorrer, sendo importante o utilizador estar atento, mantendo o antivírus atualizado, de modo a evitar que o mesmo se torne ineficaz. [4]

5 Conclusão

Como foi referido ao longo do trabalho, o software de antivírus é uma ferramenta essencial para proteger o dispositivo das diversas ameaças existentes, como vírus e malware. Por sua vez, para fazer face ao crescimento destas ameaças, que são cada vez mais sofisticadas e perigosas, torna-se importante aliar a tecnologia do software de antivírus com a inteligência artificial, de forma a maximizar a eficácia dos antivírus na deteção e eliminação do malware. Contudo, é importante que o utilizador tenha algum conhecimento sobre o funcionamento do antivírus, de modo a que procure ter sempre o dispositivo atualizado e esteja consciente das diversas limitações do mesmo.

References

[1] Xiao-bin Wang et al. "Review on the application of artificial intelligence in antivirus detection system i". In: *2008 IEEE Conference on Cybernetics and Intelligent Systems*. IEEE. 2008, pp. 506–509.

[2] Babak Bashari Rad, Maslin Masrom, and Suhaimi Ibrahim. "Evolution of computer virus concealment and anti-virus techniques: a short survey". In: *arXiv preprint arXiv:1104.1070* (2011).

[3] Rúben Manuel da Rocha Azevedo. "Propagação de vırus informáticos baseada em modelos biológicos". PhD thesis. 2013.

[4] Joxean Koret and Elias Bachaalany. *The antivirus hacker's handbook*. John Wiley & Sons, 2015.

[5] J Rosenberg. "Security in embedded systems". In: *Rugged Embed. Syst. Comput. Harsh Environ* 3.3 (2017).

[6] Davide Quarta et al. "Toward systematically exploring antivirus engines". In: *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer. 2018, pp. 393–403.

[7] Eddy Willems. "The antivirus companies". In: *Cyberdanger*. Springer, 2019, pp. 65–83.

[8] A. Newman. *How Has Antivirus Software Evolved, And Where Might The Industry Be Heading?* https://www.forbes.com/sites/forbestechcouncil/2022/03/09/how-has-antivirus-software-evolved-and-where-might-the-industry-be-heading/?sh=37d413a35e0f. Accessed: 2022-06-01.

[9] The pcInsider. *Who Invented the Antivirus? A History of Antivirus Software.* https://www.ukessays.com/essays/i technology/history-of-antivirus-software.php. Accessed: 2022-06-03.

[10] Global Data Solutions. *Quais são os 13 tipos de antivírus e como escolher o melhor?* https://gdsolutions.com.br/t de-antivirus/. Accessed: 2022-06-03.

[11] UKEssays. *History of Antivirus Software*. https://www.ukessays.com/essays/information-technology/history-of-antivirus-software.php. Accessed: 2022-06-02.