1.Spywares e Bloatwares

Spyware é um tipo de malware projetado para monitorar e registrar as atividades de um usuário sem o seu conhecimento. Esse software malicioso pode capturar informações sensíveis, exibir anúncios indesejados na tela e até mesmo desviar comissões por compras online para os atacantes. Assim como um vírus, o spyware precisa ser instalado no sistema, geralmente por meio de softwares de compartilhamento de arquivos, falsos programas de segurança ou links maliciosos enviados por e-mail. Uma vez instalado, ele pode rastrear os hábitos de navegação do usuário e enviar esses dados para servidores controlados pelos invasores. Além disso, muitos spywares incluem **keyloggers, que registram tudo o que é digitado no teclado, incluindo senhas e informações bancárias, e enviam esses registros para os criminosos**.

Felizmente, a maioria dos sistemas modernos conta com softwares antivírus e anti-malware que conseguem detectar e impedir a execução de spyware. Para minimizar os riscos, é essencial pesquisar antes de instalar qualquer programa e garantir que apenas softwares confiáveis sejam utilizados. O spyware costuma se infiltrar profundamente no sistema operacional, tornando sua remoção um grande desafio. Algumas variantes dificultam sua desinstalação, exigindo o uso de ferramentas especializadas ou até mesmo a restauração do sistema a partir de um backup seguro. Aplicações como **Malwarebytes** são especialmente projetadas para identificar e remover esse tipo de ameaça, restaurando o funcionamento normal do computador.

Outro problema que afeta muitos dispositivos é o **bloatware, que consiste em aplicativos pré-instalados pelo fabricante que muitas vezes são desnecessários**. Ao ligar um novo computador ou celular pela primeira vez, o usuário pode encontrar uma série de programas já instalados, como navegadores, ferramentas de segurança e jogos, muitos dos quais não fazem parte do sistema operacional original. Os fabricantes incluem esses softwares porque recebem incentivos financeiros das empresas responsáveis pelos programas, mas isso pode comprometer o desempenho do dispositivo e consumir espaço de armazenamento desnecessário.

Além de ocupar recursos do sistema, o bloatware pode representar um risco à segurança, pois algumas dessas aplicações podem conter vulnerabilidades exploráveis por atacantes. A melhor forma de lidar com o problema é remover manualmente os programas indesejados por meio do gerenciador de aplicativos do sistema. No entanto, nem sempre essas aplicações oferecem uma opção clara de desinstalação. Algumas exigem que o usuário localize desinstaladores específicos no menu do sistema ou no diretório do programa. Quando a remoção manual não é possível, softwares de terceiros podem ser usados para forçar a desinstalação de aplicativos persistentes.

Tanto o spyware quanto o bloatware podem comprometer a experiência do usuário e a segurança do sistema. Para se proteger, é essencial manter o sistema atualizado, utilizar ferramentas de segurança confiáveis e evitar a instalação de programas de origem duvidosa. Um gerenciamento cuidadoso de aplicativos e medidas proativas de segurança garantem que o dispositivo permaneça protegido contra ameaças digitais.

2.Spyware - Extras

Usado para coletar informações sobre um usuário e enviar as informações para outra entidade sem o consentimento do usuário. Spyware pode ser um monitor de sistema, cavalo de Tróia, Adware, cookies de rastreamento e keyloggers. O spyware pode ser instalado em um sistema por meio de downloads de software, anexos de email, links maliciosos ou explorando vulnerabilidades do sistema; uma vez instalado, o spyware monitora a atividade do usuário, coletando informações sem o conhecimento ou consentimento do usuário; as informações coletadas são geralmente transmitidas para um servidor controlado pelo atacante, onde podem ser usadas para fins maliciosos, como roubo de identidade ou fraude financeira.