1.Atualizações maliciosas

Muitas vezes ouvimos especialistas em segurança recomendam que mantenhamos nossos sistemas operacionais sempre atualizados, garantindo que todas as aplicações estejam com os patches mais recentes. Isso reduz a exposição a vulnerabilidades e problemas de segurança associados a códigos antigos. No entanto, ao instalar uma atualização, há sempre o risco de que o próprio update contenha um software malicioso. Afinal, cada vez que aplicamos uma atualização, estamos essencialmente instalando um novo software, o que pode abrir uma oportunidade para invasores injetarem código malicioso no próprio processo de atualização.

Apesar da importância de manter os sistemas atualizados, existem algumas boas práticas que devem ser seguidas para minimizar riscos. Antes de realizar qualquer modificação no sistema, é essencial ter um backup para garantir que, caso algo dê errado durante o processo, seja possível reverter a configuração anterior rapidamente. Além disso, é fundamental que as fontes das atualizações sejam confiáveis, ou seja, os arquivos devem ser baixados apenas de sites oficiais dos desenvolvedores ou de canais amplamente reconhecidos.

Um exemplo comum de atualização ocorre quando navegadores, como o Google Chrome, solicitam uma atualização automática com mensagens como: “Você está usando uma versão antiga. Atualize agora para manter seu navegador seguro e funcionando corretamente.” Se essa mensagem aparecer ao iniciar o navegador antes de acessar qualquer site, há um nível razoável de confiança de que a atualização é legítima. Porém, se esse aviso surgir após clicar em um link suspeito, pode ser um golpe de engenharia social tentando enganar o usuário para instalar um malware. Portanto, é sempre recomendável verificar se a atualização vem diretamente do site oficial.

O mesmo cuidado deve ser tomado ao baixar arquivos de atualização de terceiros. Um site desconhecido ou um pop-up inesperado sugerindo uma atualização pode ser um sinal de alerta. Sempre que possível, as atualizações devem ser obtidas diretamente da página do desenvolvedor do software. Além disso, sistemas operacionais modernos verificam assinaturas digitais antes de instalar softwares, garantindo que os arquivos realmente foram criados e assinados pelo fabricante original, como Microsoft, Adobe ou Google.

Embora a verificação de assinaturas digitais aumente a segurança do processo, ela não garante 100% de proteção contra ataques sofisticados. Um dos exemplos mais notórios desse tipo de ataque aconteceu em dezembro de 2020, quando a empresa SolarWinds revelou que seu software Orion foi comprometido. Os invasores conseguiram inserir código malicioso dentro das atualizações oficiais do software, que foram distribuídas automaticamente para usuários ao redor do mundo. Como o update

estava devidamente assinado digitalmente, parecia legítimo, levando muitas organizações a instalá-lo sem suspeitas.

O ataque ao Orion foi extremamente grave porque o software era usado por grandes empresas e agências governamentais, permitindo que os invasores acessassem redes corporativas inteiras. Como os criminosos haviam comprometido a infraestrutura de desenvolvimento da SolarWinds meses antes, suas alterações passaram despercebidas e foram distribuídas para milhares de sistemas de forma automática. Isso mostra que, embora raros, ataques baseados em atualizações comprometidas podem ter impactos massivos, permitindo que invasores espalhem malware por meio de canais confiáveis.