1.0Days

Todos os sistemas operacionais e aplicativos possuem vulnerabilidades de segurança, mesmo que ainda não tenham sido descobertas. Diariamente, pesquisadores trabalham para identificar essas falhas e comunicá-las aos desenvolvedores para que sejam corrigidas com atualizações. No entanto, hackers também buscam essas vulnerabilidades, mas com um propósito diferente: explorá-las antes que qualquer correção seja disponibilizada. Quando um atacante descobre uma falha antes da comunidade de segurança e começa a explorá-la sem que haja um patch disponível, essa ameaça é conhecida como um **ataque zero-day**.

Quando um ataque desse tipo é identificado, há uma corrida contra o tempo para desenvolver e distribuir uma atualização que mitigue a vulnerabilidade. Até que essa correção seja implementada, os atacantes podem continuar explorando a falha, tornando extremamente difícil proteger os sistemas afetados. Para acompanhar as vulnerabilidades recém-descobertas, é possível acessar o banco de dados de **Common Vulnerabilities and Exposures (CVE)**, disponível no site cve.mitre.org.

Exemplos recentes de ataques zero-day mostram a gravidade desse problema. Em abril de 2023, o Google Chrome foi alvo de um ataque que explorava corrupção de memória e um escape de sandbox. Em maio do mesmo ano, a Microsoft teve que corrigir uma vulnerabilidade crítica que permitia a execução de código assinado pelo próprio invasor durante o processo de inicialização UEFI, burlando a proteção do **Secure Boot**. Também em maio de 2023, a Apple lançou três patches emergenciais para iOS e iPadOS, resolvendo falhas que possibilitavam a execução arbitrária de código, vazamento de informações sensíveis e exploração de sandbox escape.

Muitos desses ataques zero-day já estavam sendo ativamente utilizados por criminosos, tornando essencial que as empresas de tecnologia lançassem rapidamente correções para proteger os usuários. O cenário evidencia a importância de manter os sistemas sempre atualizados e reforça a necessidade de práticas de segurança que minimizem a exposição a ameaças, como a adoção de soluções de monitoramento, o uso de autenticação multifator e a aplicação rigorosa de políticas de segurança.