Aplicativos VPN gratuitos encontrados repletos de falhas de segurança - A

Data: 2025-10-02 23:13:40

Autor: Inteligência Against Invaders

Um estudo em larga escala de aplicativos gratuitos de rede privada virtual (VPN) descobriu sérios

riscos de privacidade e segurança que afetam consumidores e empresas.

A análise, conduzida pela Zimperium zLabs, analisou 800 aplicativos VPN disponíveis para Android e iOS e descobriu que muitos não conseguiram fornecer a proteção que os usuários esperam.

Principais pontos fracos de segurança e privacidade

O relatório, *Um mergulho mais profundo: desvendando o cenário de ameaças VPN*, mostrouque os aplicativos VPN gratuitos geralmente expõem os usuários a mais perigos do que evitam.

Entre os problemas descobertos estavam bibliotecas desatualizadas, práticas de criptografia fracas, divulgações de privacidade enganosas e solicitações de permissão perigosas que se estendem muito além do que uma VPN deveria precisar.

Os pesquisadores destacaram várias descobertas preocupantes:

- Alguns aplicativos continuam a usar bibliotecas vulneráveis, como versões desatualizadas do OpenSSL, incluindo aquelas ainda suscetíveis ao infame Bug de sangramento cardíaco
- Aproximadamente 1% dos aplicativos permitiam ataques Man-in-the-Middle (MitM), que podem permitir que os invasores interceptem e descriptografem o tráfego
- Cerca de 25% dos aplicativos iOS não forneceram um manifesto de privacidade válido, um requisito fundamental sob as regras da Apple
- Muitos aplicativos solicitaram permissões excessivas, incluindo acesso a microfones, dados de localização ou logs do sistema

Leia mais sobre riscos de segurança móvel: 92% dos aplicativos móveis usam métodos criptográficos inseguros

BYOD e trabalho remoto aumentam as apostas

O estudo também alertou que as organizações com políticas de BYOD (traga seu próprio dispositivo) são especialmente vulneráveis. Mesmo aplicativos VPN amplamente baixados podem se tornar elos fracos nas defesas corporativas, potencialmente expondo dados corporativos confidenciais.

“À medida que mais funcionários trabalham remotamente em escritórios domésticos ou enquanto viajam, eles não estão apenas usando telefones pessoais, mas também laptops pessoais, muitas vezes em redes não seguras”, disse David Matalon, CEO da Venn.

“O perímetro tradicional se foi, e a realidade de BYOD (traga seu próprio dispositivo) para trabalhadores remotos requer uma mudança de estratégia: de proteger o dispositivo para proteger o trabalho em si.”

Matalon acrescentou: “As VPNs continuam a desempenhar um papel vital na proteção e anonimização das conexões de rede, no entanto, podem fornecer uma falsa sensação de segurança e privacidade do usuário”.

Ele enfatizou que os aplicativos VPN de nível de consumidor e as extensões de navegador geralmente carecem de auditorias, deixando os usuários vulneráveis a criptografia fraca e as empresas em risco de perda de dados.

Uma mudança para modelos de segurança mais fortes

No iOS, mais de 6% dos aplicativos foram encontrados solicitando direitos privados – permissões que podem permitir acesso profundo ao sistema operacional.

Embora não esteja claro se esses pedidos foram atendidos, as descobertas sugerem baixa adesão às diretrizes de segurança da Apple.

“As organizações precisam de uma resposta em várias camadas”, disse Brandon Tarbet, diretor de TI e segurança da Menlo Security.

“A visibilidade e o gerenciamento de endpoints são apostas de mesa […] O que está rapidamente se tornando um requisito é a necessidade de segurança de dados em nível de conteúdo da web.”

James Maude, CTO de campo da BeyondTrust, apontou que “as tecnologias VPN há muito apresentam desafios de segurança para as organizações em uma era de ataques e comprometimentos de identidade”.

Ele enfatizou que as abordagens de confiança zero são vitais, pois o acesso VPN comprometido pode expandir o alcance de um invasor pela rede.

Vishrut Iyengar, gerente sênior de soluções da Black Duck, acrescentou que os dispositivos móveis agora são o principal alvo.

“Hoje, estamos enfrentando uma realidade preocupante de que muitos aplicativos móveis corporativos ainda carecem de proteções básicas, como ofuscação de código, armazenamento seguro e bibliotecas de terceiros atualizadas”, explicou.

Finalmente O estudo conclui que muitas VPNs gratuitas oferecem pouca segurança real. Em vez disso, eles podem servir como veículos para vigilância, roubo de credenciais e até mesmo comprometimento total do dispositivo.